Legal-URN Framework for Legal Compliance of Business Processes

by

Sepideh Ghanavati

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the Ph.D. degree in
Computer Science

Ottawa-Carleton Institute for Computer Science
Faculty of Graduate and Postdoctoral Studies
University of Ottawa

Abstract

In recent years, the number of regulations an organization needs to comply with has been increasing, and organizations have to ensure that their business processes are aligned with these regulations. However, because of the complexity and intended vagueness of regulations in general, it is not possible to treat them the same way as other types of requirements. On the other hand, the cost of being non-compliant can also be fairly high; non-compliance can cause crucial harm to the organization with financial penalties or loss of reputation. Therefore, it is very important for organizations to take a systematic approach to ensuring that their compliance with related laws, regulations and standards is established and maintained.

To achieve this goal, this thesis proposes a model-based compliance analysis framework for business processes called Legal-URN. This framework is composed of four layers of abstraction linked to each other. The framework exploits the User Requirements Notation (URN) as the modeling language to describe and combine legal and organizational models. In order to model legal documents, legal statements are first classified into four classes of Hohfeldian rights, and then Hohfeldian models of the regulations and their statements are created. These models are further refined into legal goal and business process models via a domain-specific version of URN called *Legal URN profile*. To check the well-formedness of the models and to identify instances of non-compliance, 23 Object Constraint Language (OCL) rules are provided. In this thesis, the quantitative and qualitative analysis algorithms of URN's Goal-oriented Requirement Language are extended to help analyze quantitatively and qualitatively the degree of compliance of an organization to the legal models. Furthermore, with the help of a prioritization algorithm, the framework enables one to decide, while taking the organization goals into consideration, which non-compliant instances to address first in order to provide a suitable evolution path for business processes.

In addition, to assess compliance with more than one regulation, a pair-wise comparison algorithm enables organizations to identify the similarities and conflicts among

regulations and incorporate them in the models. The jUCMNav tool, an Eclipse plug-in for URN modeling and analysis, was extended to support the framework and its algorithms and rules.

The thesis contributions are evaluated through a gap analysis based on a systematic literature review, a comparison with closely related work, and two case studies in the healthcare domain: one with a single regulation and realistic business processes, and a second with three additional regulations. We also identify the benefits and limitations of the framework, as well as potential extensions for future work.

The Legal-URN framework provides a tool-supported, rigorous approach to compliance analysis of organizations against relevant regulations.

Acknowledgements

First and foremost, I would like to thank both my supervisors, Dr. Daniel Amyot and Dr. Liam Peyton, for their most valuable, motivating and productive guidance and research work throughout the last few years. I also would like to thank my committee members for accepting to review this work and for providing me with constructive comments and feedback.

This work would not have been possible without the collaboration and discussions I was lucky to have with many co-authors and researchers around the world (too many to mention them all). However, I want to especially thank the Software Engineering research group at Fondazione Bruno Kessler (FBK), Trento, Italy, and more specifically Dr. Angelo Susi, Dr. Anna Perini and Dr. Alberto Siena, for giving me the opportunity to collaborate with them and for making me feel at home while visiting Trento.

I owe major thanks to the system support and administration staff of the School of Electrical Engineering and Computer Science, and especially to Jacques Sincennes.

I am thankful to the many organizations and agencies that have funded my research and travels over the years: the National Science and Engineering Research Council (NSERC) for a Canada Graduate Scholarship and the Michael Smith Foreign Study Supplement, the Ontario Graduate Scholarships program, NSERC's Business Intelligence Network (BIN), the NSERC/CIHR Collaborative Health Research Program (CHRP), and the Ontario Research Network for Electronic Commerce (ORNEC). Many thanks also to the University of Ottawa for an admission scholarship and for travel grants.

I would also like to thank my family and my friends from all over the world (there are many of you – you know who you are!) for their constant support, especially my parents, my grandparents and my sister for their understanding throughout my studies, and all the people who were involved in our research team.

Finally, thank you Manuel for all the support in the last and hardest year of my PhD. Without you I wouldn't be able to make this happen.

Contents

List of Tables

List of Figures

List of Acronyms

ACM	Association for Computing Machinery
AR	Access-Right
BP	Business Process
BPM	Business Process Modeling
BPMN	Business Process Model and Notation
CAiSE	International Conference on Advanced Information Systems Engineering
CSV	Comma-Separated Value
DOR	Delegation of Authority Right
ERM	Enterprise Risk Management
FCL	Formal Contract Language
FIPPA	Freedom of Information and Protection of Privacy Act
GBRAM	Goal-Based Requirements Analysis Method
GEM	Government Extraction Model
GORE	Goal-Oriented Requirements Engineering
GRL	Goal-oriented Requirement Language
GS	Google Scholar
HCCA	Health Care Consent Act
HIC	Health Information Custodian
HIPPA	Health Insurance Portability and Accountability Act
IEEE	Institute of Electrical and Electronics Engineers

IPCF	Indicator-based Policy Compliance Framework
IQS	Improve Quality of Services
IS	Information Systems
ITU	International Telecommunications Union
IUPH	Increase Understanding of Public Health
jUCMNav	Java Use Case Map Navigator
KPI	Key Performance Indicator
MC	Minimizing Cost
MFIPPA	Municipal Freedom of Information and Protection of Privacy Act
NFR	Non-Functional Requirement
OCL	Object Constraint Language
PAL	Privacy Analysis Language
PAT	Privacy Analyzer Tool
PBH	Provide Better Healthcare
PGMT	Privacy Goal Management Tool
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PI	Personal Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PPC	Protect Privacy and Confidentiality of PHI
QoCIPA	Quality of Care Information Protection Act
RE	Requirements Engineering
REB	Research Ethics Board
REJ	Journal of Requirements Engineering
RELAW	Requirements Engineering and Law
RLNS	Restricted Natural Language Statements
RSL	Requirements Specification Language
SC	Scopus

SD	Strategic Dependency
SL	SpringerLink
SOC	Separation of Concerns
SR	Strategic Rationale
UCM	Use Case Maps
UML	Unified Modeling Language
URN	User Requirements Notation

Chapter 1

Introduction

1.1 Motivation

With the rapid increase and evolution of regulations and policies relevant to business processes, it becomes difficult for organizations to constantly keep their goals, policies and business processes compliant with applicable legislation. These concerns are especially evident in fields related to environmental issues or privacy in healthcare and communications, where new laws and regulations are frequently introduced, in addition to new versions of existing ones. Furthermore, the legal documents that dictate how a corporation must behave are usually complex. This complexity originates from: having many cross-references to other parts of the same legal document and to other related regulations; the inherent vagueness of legal documents because they aim to cover all situations while remaining fairly susceptible to amendments and updates; and the fact that these documents are constantly changing. The end result is that the analysis of legal documents is difficult for organizations to handle and techniques are needed to enable useful analysis in this context.

Organizations are motivated to comply with legislation since failure to do so leads to undesirable consequences usually in the form of financial penalties, loss of reputation and lawsuits. Such consequences may hurt the ability of an organization to fully achieve

its corporate mission and objectives. Also, the different stakeholders in an organization may introduce goals that conflict with existing ones or with each other. These goals may even unknowingly conflict with the law. Consider as well that being fully compliant with legislation (some of which may be optional) may not be in the organization's best interests or even a feasible option. In such cases, the best situation is to be able to identify and achieve a set of high-level goals. Organizations may wish to consider alternative solutions based on these top-level goals and aim for minimum compliance with the law. Some organizations even opt to pay penalties if it proves cost effective to do so at a given point in time.

For the reasons stated above, organizations need to implement a systematic approach and leverage tool support in order to manage and maintain compliance of their business processes and goals in a continuous fashion. It is also necessary for them to be able to analyze, address and resolve potential instances of non-compliance. To avoid the negative consequences of non-compliance, it is necessary for an organization to be able to track its overall compliance with regulations and provide a detailed compliance check for its individual business processes. Finally, to estimate risk and demonstrate progress towards complete compliance, it is necessary to be able to report a degree of compliance. Different organizations have different requirements and different degrees of maturity, and hence such reporting can be done either quantitatively or qualitatively.

With respect to achieving these objectives and addressing the problem of compliance, there are several tasks an organization must coordinate. These include:

1. Keeping track of which regulations are relevant.
2. Identifying which parts of regulations are relevant to which business processes.
3. Extracting relevant legal requirements from source documents.
4. Identifying instances of non-compliance and prioritizing them for resolution.
5. Identifying conflicting goals between stakeholders and within legal documents.

6. Resolving conflicts and satisfying goals.

7. Defining the overall and individual degree of compliance quantitatively or qualitatively.

8. Ensuring that the relevant legal requirements are integrated into the business processes and that the overall business strategy is optimized.

9. Resolving cross-references.

10. Updating and managing all of the above in the face of ongoing evolution of business goals, business processes, and applicable regulations.

In recent years, much effort has been invested in Computer Science, specifically in the fields of Requirements Engineering, Logic and Natural Language Processing, to solve some of the issues mentioned above. As Otto et al. observe [83], some researchers exploit the benefits of requirements-oriented methodologies [26, 30, 87, 101], some use different types of logics such as symbolic logic, deontic logic, first-order temporal logic, or defeasible logic [1, 5, 8, 9, 12, 36], while others use methodologies based on the analysis of natural language [14, 55, 64].

Requirements Engineering (RE) approaches focus on the fact that legal statements can be treated as a type of requirement. These approaches aim to integrate laws with other types of requirements so that they can be modeled using the same notation or language. The idea is that if the notation used for the model of laws is the same as other types of requirement models, then the total comprehensibility of the union of both models will increase and more sophisticated analyses for compliance and business strategies become possible. With RE techniques, change management can be performed through links between elements of the model. RE approaches can be both graphical and textual, making it possible to integrate logical aspects with RE languages and make use of logical approaches for legal compliance. However, RE languages have not been typically developed to support the level of complexity that exists in the law. This is because

requirements are usually intended to be written as single clear statements whereas laws intend to cover all circumstances with as few specifics as possible. Therefore, it has become necessary to explore the possibility of creating extensions to current modeling languages in order to be able to support all aspects of legal documentation.

One type of approach in RE, which has attracted much attention in the domain of legal compliance over the years, is goal-oriented modeling [11, 25, 103, 101]. Since goal-oriented modeling notations are used to capture goals that are high-level, generic and abstract in nature, they are well-suited for modeling legal statements.

An early attempt at creating a requirements management framework for use by an organization in the modeling of legal documents and the management of compliance is proposed in [24, 25]. This framework uses the User Requirements Notation (URN) standard [53]. This standard combines the Goal-oriented Requirement Language (GRL) with the Use Case Map (UCM) scenario notation. The unique characteristics of this framework are:

- Using the same, standardized language for modeling business processes, goals and legislation.
- Providing traceability between business processes, goals and legal documents.
- Identifying instances of non-compliance through traceability links.
- Managing the evolution of both law and organizational goals and processes via traceability links.

Although this simple framework helps to find instances of non-compliance and identify a set of activities needed to reach full compliance, portions of the law may not be relevant given a particular organization's context and there is no support for the different priorities of the resulting activities. There are also no guidelines on how to extract these goals and thus there is no way to analyze the degree of compliance quantitatively

or qualitatively. Methods for prioritizing instances of non-compliance, handling of cross-references, conflicts and multiple laws are absent. This framework will however provide a useful basis for our current work towards full consideration of techniques required for legal compliance.

In the following sections we will provide more details on the exact contributions of this thesis as well as on the research methodological used.

1.2 Research Hypothesis

With respect to the real-world needs and the limitations of existing frameworks stated in Section 1.1, we aim to answer the following questions in this thesis:

1. How can relevant legal models be extracted from source documents?
2. How can organizations ensure their business processes and goals are compliant with legal documents?
3. How can instances of non-compliance be identified and prioritized?
4. How can multiple laws be considered, and conflicts between the stakeholder's goals and the laws be handled?

Our hypothesis is that a goal-oriented compliance framework for managing and maintaining business process compliance can help answer these questions. Our novel framework, called Legal-URN, supports a more systematic modeling and analysis of compliance issues. It can help organizations (and legislators) avoid expensive and damaging compliance breaches. The Legal-URN framework also aims to bridge the gap between the abstract level of legal prescriptions and the concrete task level that resides within business processes. The framework includes four layers:

- The legal and business process documents (usually in textual form).

- Legal statements classified according to different classes of rights.
- GRL models describing the law and the organization's objectives.
- Business processes and process-level legal prescriptions modeled with UCM.

Note that this approach substantially extends the ideas found in [24, 25]. However, it does not revisit explicitly how to maintain the compliance of business processes when a change to either the organization or the law occurs. The approach of [24, 25], which exploits a Requirements Management System (e.g., IBM DOORS) to manage such changes, can be reused as is for the new Legal-URN framework.

1.3 Thesis Methodology

In this thesis, we follow a design-oriented research approach proposed by Hevner et al. [47] and Oates [82]. In design-oriented approaches, defining a problem domain and its solution is achieved through building the designed artifacts and evaluating those artifacts. A design-oriented approach usually starts with an initial literature review on a designed artifact, followed by steps for identifying the problem, designing the research, completing a thorough literature review and identifying the current state-of-the-art, developing the framework (research rigor), evaluating the framework (via case studies, field studies, analytical studies, etc.), and improving and re-evaluating the framework. Figure 1.1 shows these steps.

We aim to develop a framework that satisfies the questions presented in Section 1.2 and the overall objectives in Section 1.1. For this, we first identify the problem and the potential solutions and scenarios we want to offer. We also perform a gap analysis of the approaches that exist in the literature through a systematic literature review inspired from the approach of Loniewski et al. [68], itself based on Kitchenham's [58]. Next, we develop our *initial* framework and algorithms iteratively to cover the gaps identified in a first case study. In this phase, we evaluate our solution against the current

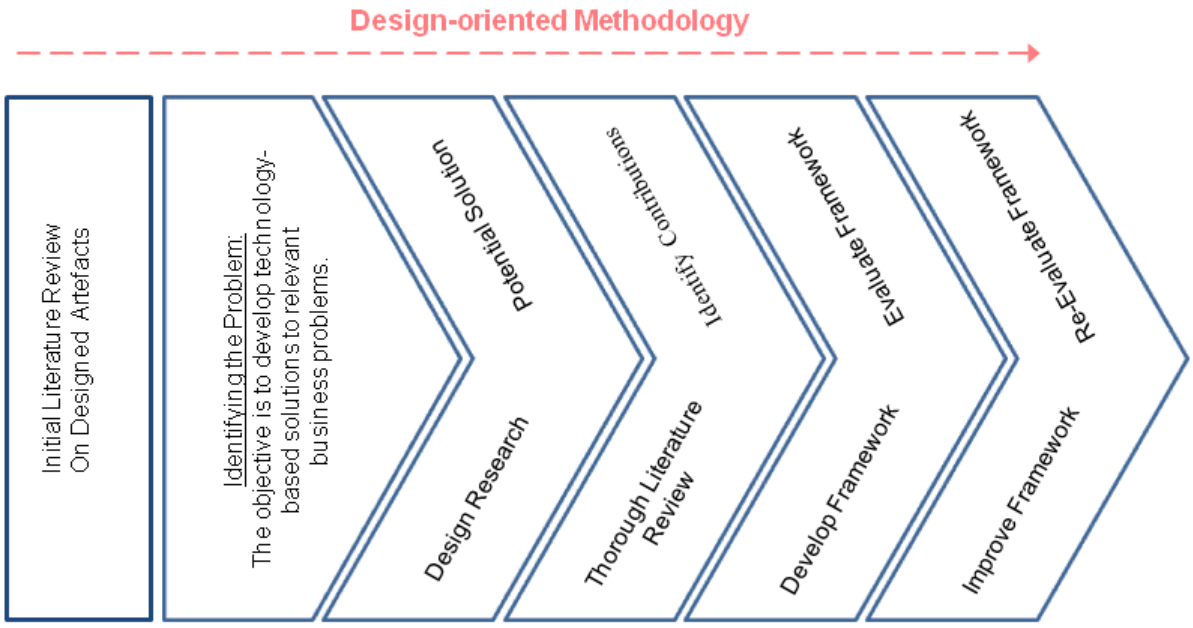

Figure 1.1: Design-oriented Approaches

literature and identify any gaps remaining (which are mainly related to the handling of multiple regulations). Then, we *refine* the framework to address those gaps and validate it via another case study. Finally, we evaluate our framework using five different methods. The first method is a gap analysis between what is needed and what the literature currently offers, together with a comparison to our Legal-URN framework capabilities. The second and third methods involve comparisons between Legal-URN and two closely related approaches, namely plain URN and Shamsaei's Indicator-based Policy Compliance Framework [95], which is also based on URN. The fourth one is the evaluation based on the two case studies and finally the fifth and last method focuses on the automation of the framework steps with tool support.

1.4 Thesis Contributions

Major Contributions

The thesis make two major contributions:

1. The LEGAL-URN framework itself, which helps model legal and organizational documents in the same notation, analyze the compliance, manage compliance and evolution of laws and business processes, identify non-compliant instances and prioritize non-compliance issues. The LEGAL-URN framework uses four layers for the legal model. The LEGAL-URN framework covers the following sub-contributions:

   (a) A meta-model formalizing the concepts of the framework.

   (b) The implementation of the meta-model with URN through a lightweight profile supporting compliance analysis and legal aspects by defining a set of new goal stereotypes (namely consequences, obligations, permissions, preconditions, XRef, exceptions, no and no-precondition) and link stereotypes. This extension is called Legal URN profile.

   (c) Definition of guidelines to map legal documents/statements to a Legal URN model.

   (d) Improvement of the existing GRL analysis algorithms to enable quantitative and qualitative analysis while computing degrees of compliance of an organization to the law and identifying instances of non-compliance.

   (e) Provision for a methodology and algorithms to prioritize an organization's instances of non-compliance to the law.

   (f) Definition of a set of formal rules to ensure the well-formedness of the Legal URN models and examine their compliance automatically.

   (g) Definition of the steps needed to build and exploit Legal URN models for compliance.

2. Modeling and analysis of common cases encountered when complying with multiple laws/regulations. The approach, also part of the LEGAL-URN framework, enables the modeling of relationships between legal models and their exploitation and reuse by multiple organizations.

Minor Contributions

The following minor contributions are also made in this thesis:

1. A systematic review of goal-oriented requirements management frameworks for business process compliance using 88 publications selected from five search engines and from the study of specialized conferences.

2. Extension of the current jUCMNav tool to support the new domain-specific URN customizations (Legal URN profile) for compliance, as well as the well-formedness and analysis rules (implemented with the Object Constraint Language – OCL), and the new GRL analysis algorithms.

3. Case studies aiming to validate this framework. The second case study is the only one, to our knowledge, that uses a goal-oriented compliance modeling approach to explicitly handle multiple regulations.

Note that the qualitative and quantitative algorithms for the analysis of GRL models, to be reviewed in Section 2.4.2, together with an improved version of Roy's original hybrid algorithm [90] and their implementation in jUCMNav, were also contributed by me as part of a Directed Studies course during my Ph.D. studies. The three algorithms are now part of the URN standard itself [53], and they are used by thousands of people around the globe. These algorithms are also explained in a journal paper [2] already cited 47 times in the past two and a half years. This thesis further extends these algorithms to handle compliance assessments, in a backward compatible way (i.e., the new algorithms work the same way as before on non-Legal-URN models).

1.5 Publications Based on Thesis

Various aspects of this thesis have led to many publications, where the first author is the main author:

Refereed Book Chapter

1. A. Pourshahid, L. Peyton, S. Ghanavati, D. Amyot, P. Chen, M. Weiss (2012) Model-Based Validation of Business Processes. In: V. Shankararaman, J.L. Zhao and J.K. Lee (Eds) *Business Enterprise, Process, and Technology Management: Models and Application.* Business Science Reference, IGI Global, USA, 165–183, DOI: 10.4018/978-1-46660-249-6.

Refereed Journals

2. S. Ghanavati, A. Siena, D. Amyot, A. Perini, L. Peyton, and A. Susi (2010) Integrating Business Strategies with Requirement Models of Legal Compliance. *Int. Journal of Electronic Business*, Inderscience Publishers, Vol. 8, No. 3, 2010, 260–280.

3. D. Amyot, S. Ghanavati, J. Horkoff, G. Mussbacher, L. Peyton and E. Yu (2010) Evaluating Goal Models within the Goal-oriented Requirement Language. *Int. Journal of Intelligent Systems (IJIS)*,Vol. 25, Issue 8, August 2010, 841–877.

4. A. Pourshahid, P. Chen, D. Amyot, A.J. Forster, S. Ghanavati, L. Peyton and M. Weiss (2009) Business Process Management with the User Requirements Notation. *Electronic Commerce Research*, 9(4), Springer, December 2009, 269–316.

Refereed Conferences and Workshops

5. A. Rifaut, and S. Ghanavati (2012) Measurement-Oriented Comparison of Multiple Regulations with GRL. *5th Int. Workshop on Requirements Engineering and Law*

(RELAW), Chicago, USA, September. IEEE CS, 7–16.

6. S. Ghanavati, D. Amyot, and L. Peyton (2011) A Systematic Review of Goal-oriented Requirements Management Frameworks for Business Process Compliance. *4th Int. Workshop on Requirements Engineering and Law (RELAW)*, Trento, Italy, August. IEEE CS, 25–34.

7. D. Amyot, G. Mussbacher, S. Ghanavati, and Kealey, J. (2011) GRL Modeling and Analysis with jUCMNav. *5th Int. i* Workshop*, Trento, Italy, August. CEUR-WS, Vol-766, 160–162.

8. S. Ghanavati, A. Siena, D. Amyot, A. Susi and A. Perini (2010) Towards a Framework for Business Process Compliance. *Goal-based Business Process Engineering (WGBP'10)*, Vitoria, Brazil, October. IEEE CS. DOI:10.1109/EDOCW.2010.46

9. S. Ghanavati, A. Siena, D. Amyot, A. Susi and A. Perini (2010) Making Business Processes Law-Compliant. *1st Workshop on Law Compliancy Issues in Organisational Systems and Strategies (iComply'10)*, Fiesole, Firenze, Italy, July.

10. S. Ghanavati, D. Amyot and L. Peyton (2009) Compliance Analysis Based on a Goal-oriented Requirement Language Evaluation Methodology. *17th IEEE Int. Requirements Engineering Conference (RE'09)*, Atlanta, USA, September. IEEE CS, 133–142. *(Acceptance rate: 21%)*

11. S. Ghanavati, A. Siena, A. Perini, D. Amyot, L. Peyton and A. Susi (2009) A Legal Perspective on Business: Modeling the Impact of Law. *4th International MCeTech Conference on eTechnologies*, Ottawa, Canada. LNBIP 26, Springer, 267–278.

12. S. Ghanavati, D. Amyot, and L. Peyton (2008), Comparative Analysis between Document-based and Model-based Compliance Management Approaches. *First Int. Workshop on Requirements Engineering and Law (RELAW)*, Barcelona, Spain, September. IEEE CS, 35–39.

13. Pourshahid, D. Amyot, L. Peyton, S. Ghanavati, P. Chen, M. Weiss, A. Forster (2008), Toward an integrated User Requirements Notation framework for Business Process Management. *3rd Int. MCeTech Conference on eTechnologies*, Montreal, Canada. IEEE CS, 3–15. *(Best Paper Award)*

Peer-Reviewed Research Demos

14. G. Mussbacher, S. Ghanavati, and D. Amyot (2009) Modeling and Analysis of URN Goals and Scenarios with jUCMNav. Research demo, *17th IEEE Int. Requirements Engineering Conference (RE'09)*, Atlanta, USA, September. IEEE CS, 383–384.

1.6 Thesis Outline

This thesis is structured as follows. Chapter 2 provides an overview of business process legal compliance and legal statement ontologies, URN (GRL, evaluation algorithms, and UCM), other goal modeling notations and another goal-based legal framework (*Nómos*). Chapter 3 presents the results of our systematic literature review. Chapter 4 discusses the details of the Legal-URN framework, the tailoring of URN for compliance, and an overview of the steps for compliance analysis. Chapter 5 explains the rules for compliance and their well-formedness. The chapter also describes our quantitative and qualitative compliance analysis approach as well as the prioritization algorithms. Chapter 6 presents our first case study, the business process compliance of a hospital in Ontario against one privacy law. Chapter 7 discusses additional literature review for handling multiple legislation and describes an approach to handle multiple laws in the Legal-URN framework. Chapter 8, covers the second case study, which extends the first one by adding three more regulations with which the organization must comply. Chapter 9 discusses the evaluation of the framework based on the literature survey, closely related work, the two case studies, and tool support. Finally, in Chapter 10, we present our conclusions and items for future work.

Note that the thesis also contains five appendices:

A. The list of papers used in the systematic literature review.

B. The well-formedness and compliance rules formalized in OCL.

C. Parts of the Hohfeldian and GRL models of the law used for the first case study (PHIPA).

D. The GRL and UCM models and the results of the legal compliance analysis of the organization (The Ontario Hospital) used in the first case study.

E. Parts of the legal models for additional regulations used in the second case study (Qo-CIPA and FIPPA), together with an analysis of relationships between the regulations involved.

Chapter 2

Background

In this chapter, we provide an overview of background concepts and notations related to this thesis. First, we define business processes, legal compliance for business processes, regulations, as well as different regulation taxonomies used to extract elements of right exist in the regulations. Then, we introduce the User Requirements Notation (URN) with some examples. In our work, we use and extend URN for modeling legal requirements and analyzing legal compliance. We also explain other relevant goal modeling notations found in Requirements Engineering that could represent potential alternatives for the goal modeling notation we adopt in our framework. Finally, we provide an overview of the Nòmos framework, which includes a modeling notation for legal documents, and discuss the definitions we adopt from this framework.

2.1 Legal Compliance and Business Processes

A business process is a set of activities performed by people, organizations or machines to reach a business goal or achieve a business result [85]. Business processes can also include multiple sub-processes, and they can be automated or manual. Business processes can be restricted to one unit of an organization or span different units of a single organization or even different organizations.

To represent their current and future business processes, organizations can use Business Process Modeling (BPM) methodologies. With such methodologies, it is possible to develop a basis for integrating various stakeholder objectives and for improving business processes and their activities to achieve business goals.

Business processes define flows of activities inside an organization to fulfill a set of goals. Thus, they highly depend on data related to those activities to perform properly. However, accessing this data needs to be done with careful attention in order to avoid any breach of privacy. To protect privacy, several regulations, such as those found in the financial or healthcare sectors, have been introduced by governments. Organizations, hence, have to ensure that their goals and business processes are compliant with these regulations. However, as mentioned in Chapter 1, there can be more than one regulation or standard relevant to an organization and it is necessary for organizations to be able to identify these regulations properly. Furthermore, these regulations can conflict with each other, e.g., some can have stricter rules or different time-lines than others.

2.2 Regulations and Ontologies

2.2.1 Definition of Legal Documents

Legal documents contain sets of rule statements that are imposed by governments. Organizations are required to comply with these regulations as otherwise they would face negative consequences such as financial penalties, lawsuits, or loss of reputation. Legal documents mainly address actors, obligations, and permissions [14]. They may also include some exceptions, constraints, or conditions. Some examples of such legal documents are:

- Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada [37]
- Personal Health Information Protection Act (PHIPA) - Ontario [40]
- Health Insurance Portability and Accountability Act (HIPAA) - USA [106]

- Data Protection Directive - European Union [112]

2.2.2 Legal Ontologies

Legal statements have been categorized in different ways by different taxonomies or ontologies. Taxonomies are hierarchical relationships, whereas ontologies are more general (akin to meta-models). A taxonomy can be seen as an ontology mainly composed of *is-a* relationships. There are several taxonomies for classifying legal statements, however we only focus on a few here.

One of the taxonomies is based on *Deontic Logic* [7, 50]. In deontic logic, legal statements are classified as *Obligations*, *Permissions*, and *Interdictions*. According to Barbuceanu [7], an obligation imposed on an agent is defined as an action that will incur a cost on the agent when the action is not performed. An interdiction is an action that will incur a cost when it is performed, whereas a permission is an action that is likely desirable but that will not result in any cost when it is not performed. An interdiction can also be interpreted as the obligation of *not* performing an action, whereas a permission is equivalent to not being interdicted to perform an action. Note that "performing an action" is mostly from an operational perspective; obligations, interdictions, and permissions also apply to contexts where statements discuss "meeting objectives", "reaching a specific state", etc.

Another way of classifying legal statements is based on the *Hohfeldian* taxonomy of rights (Hohfeld, 1913) [111]. In the Hohfeldian taxonomy, as expressed by Siena [99], a *right* can be one of the following: duty, privilege, claim, no-claim, power, immunity, liability, and disability. This taxonomy also corresponds to the definition of Hohfeldian notions from Sartor [93] and Logrippo [67]. Sartor and Logrippo classify rights as: duty, privilege, right, noright, power, immunity, subjection, and disability. In this thesis, however, we adopt Siena's terminology, for consistency.

In [93], Sartor categorizes the first four classes of rights as "obligative statements" and the last four classes of rights as "potestative statements". An obligative statement means

that the actor j has an obligation towards the actor k. The negation of this statement provides us with the definition of privilege, which means that the actor j has no obligation towards the actor k. In potestative statements, the actor j has a power to make actor k perform an action that has been forbidden. These two types of statements build the two Hohfeldian squares, which include correlative and opposite rights. Two rights are correlative if a right for a person implies another right for the other person. Two rights are opposite if the existence of one right excludes the existence of the other right. Correlative rights with respect to the Hohfeldian taxonomy and [93] are Duty-Claim, Privilege-NoClaim, Power-Liability, and finally Immunity-Disability. The definitions of these correlative rights are as followed:

- **Duty-Claim.** Duty means that actor j is obliged to perform an action that actor k asks for. This implies that actor k can "claim" from actor j to perform an action.
- **Privilege-NoClaim.** Privilege is the right where actor j has a permission to perform an action for actor k whether or not actor k claims for it. This means actor k cannot claim from actor j to perform that action.
- **Power-Liability.** Power is the ability of actor k to achieve an action B by making actor j perform an action A. Actor j has the corresponding liability (i.e., responsibility) in return.
- **Immunity-Disability.** Immunity is a defense of an actor against others' capability to penalize that actor. Immunity means that the actor has no liability to perform an action [76]. The counterpart actors will be disabled from any penalization action and are free from legal power.

Another classification of legal statements has been introduced by Breaux et al. [14]. According to these authors, legal statements are types of rights, obligations, and constraints. Rights are claims that are assigned to the right-bearer while obligations are duties that must be fulfilled to be compliant with regulations. The actor of the right

and the actor of the obligation are complementary. In this classification, constraints are preconditions, exceptions, or dependent obligations and rights. Any legal statement can be illustrated as an obligation or right statement with some constraints.

In our work, we first identify Hohfeldian rights in the legal statements and then map these classes of rights to the deontic modalities' types of statements.

2.3 Goal-Oriented Requirements Engineering

Requirements Engineering (RE) is concerned with the elicitation, analysis, specification, validation, and management of requirements. One of the main approaches in RE is Goal-Oriented Requirements Engineering (GORE), which aims to elicit, analyze, and describe stakeholder requirements as goals. This approach provides new types of analyses for non-functional requirements and helps document the rationale behind such requirements. GORE processes cover both bottom-up and top-down approaches. Bottom-up approaches usually start from concrete scenarios while top-down approaches start from abstract concerns and objectives. In GORE, goals range from high-level strategic objectives to low-level technical tasks assigned to actors. Goal models are used to refine high-level goals into other goals and low-level operationalized tasks, to find alternatives for achieving goals, and to assign tasks to actors [61]. Goals can also be categorized as functional or non-functional. Functional goals are often used to model elements of uses cases and state machines while non-functional goals are used to capture desired qualities.

In the last 20 years, various goal-oriented notations such as the NFR Framework [16, 81], *i** [115, 117, 116], KAOS [19], Tropos [31] and the Goal-oriented Requirement Language (GRL) [2] have been introduced. All of these notations have some tool support available for the modeling and analysis of goals, alternatives, and rationales.

In Section 2.4, we explain the User Requirements Notation [53], which includes GRL and Use Case Maps (UCMs), together with algorithms for evaluating GRL models and tool support for modeling and analyzing URN models. In Section 2.5, we describe other

popular goal modeling languages, often in contrast to GRL.

2.4 User Requirements Notation

The User Requirements Notation [53] is a recent Recommendation of the International Telecommunications Union (ITU-T) that allows software and requirements engineers to discover and specify requirements for a proposed or an evolving system, and analyze such requirements for correctness and completeness. URN combines the *Goal-oriented Requirement Language* for modeling goal-oriented and intentional concepts (related to non-functional requirements, quality attributes, and reasoning about alternatives) with the *Use Case Map* notation for modeling scenario concepts (related to operational requirements, functional requirements, and performance and architectural reasoning). In particular, URN has concepts for the specification of stakeholders, goals, non-functional requirements, rationales, behavior, scenarios, scenario participants, and high-level architectural structure [4].

GRL includes intentional elements (i.e., goals, softgoals, tasks and resources) as well as different links that connect these elements to each other. These links represent different types of relationships such as contributions, correlations, decompositions and dependencies. UCM focuses mainly on the functional or operational requirements of a system and the causal relationships between the responsibilities of different use cases. UCM can be used to model business processes as well as to capture, elicit and validate use cases. With these two complementary views, URN also allows for the alignment of business goals and business processes.

2.4.1 Goal-oriented Requirement Language

The Goal-oriented Requirement Language is a goal modeling notation that combines several concepts borrowed from i^* and the NFR Framework. According to Amyot et al. [3], GRL has several benefits over other popular goal modeling notations, including:

- Its integration with a scenario notation (UCM).
- Its support for qualitative and quantitative attributes (for contributions levels and satisfaction levels)
- A clear separation of GRL model elements from their graphical representation.
- Its support for providing a scalable and consistent representation of multiple views/-diagrams of the same goal model.
- Its support for evaluation strategies as part of the model.
- Its support for tailoring the language to particular domains via metadata, URN links, and OCL constraints.

The syntax of GRL is based on the syntax of the *i** language. A GRL diagram shows the high-level business goals and non-functional requirements of interest to stakeholders and the alternative means for achieving these goals and requirements. A goal diagram also documents beliefs (facts) important to stakeholders, as well as stakeholder dependencies.

GRL intentional elements can be softgoals ( , e.g., Improve Quality of Care in Figure 2.2), goals ( , e.g., Do Research), tasks ( , e.g., Access Patient PHI), beliefs or resources (). Softgoals differ from goals in that there is no clear, objective measure of satisfaction for a softgoal whereas a goal is quantifiable (often in a binary way) and can be fully met. Often, softgoals are related to non-functional requirements and qualities, whereas goals are related to functional requirements. Tasks represent solutions to goals or softgoals. Resources are sometimes necessary to be able to achieve tasks, goals and softgoals.

An actor ( , e.g., Researcher) represents a stakeholder of the system or another system. Actors are active entities in the system who want goals to be achieved, tasks to be performed, resources to be available and softgoals to be satisfied.

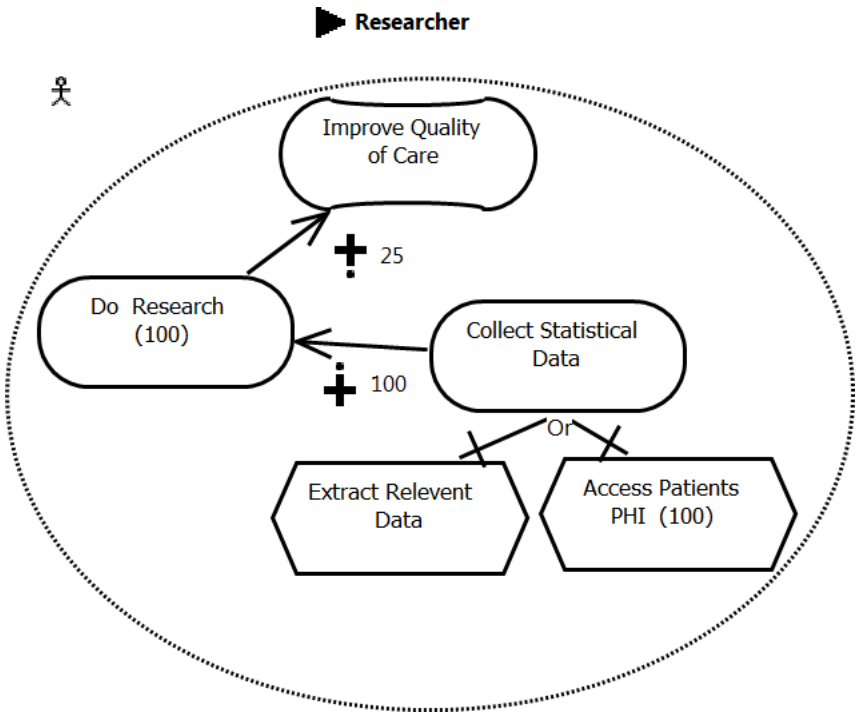

Figure 2.1: GRL Model Example

GRL intentional elements are connected to each other through decomposition (⊢—), contribution (⟶), correlation (⇢) or dependency (—●—) links. Decomposition links allow an element to be decomposed into sub-elements. A decomposition can be a type of AND, IOR, or XOR. XOR and IOR decomposition links and may alternatively be displayed as *means-end* links. Contribution links indicate the impact of one element's satisfaction on another element's satisfaction. A contribution link can have a qualitative contribution level, qualitativeContribution (*make*, *help*, *some positive*, *none*, *some negative*, *hurt* and *break*), or a quantitative contribution level, quantitativeContribution (an integer value between -100 and 100). Correlation links are similar to contribution links, but describe side-effects rather than desired impacts. Finally, dependency links model relationships between actors (one actor depending on another actor for something specified with an intentional element).

GRL supports different *evaluation mechanisms* that enable modelers to analyze the most appropriate trade-offs among (often conflicting) goals of stakeholders. GRL evalu-

ations are bottom-up, and they make use of GRL *strategies*. The next section explains the GRL evaluation algorithms that we developed as part of a directed study course in 2007. These algorithms are now part of the URN standard itself.

Figure 2.1 shows an example of a small GRL model whereas Figure 2.2 recalls the basic elements of the GRL notation.

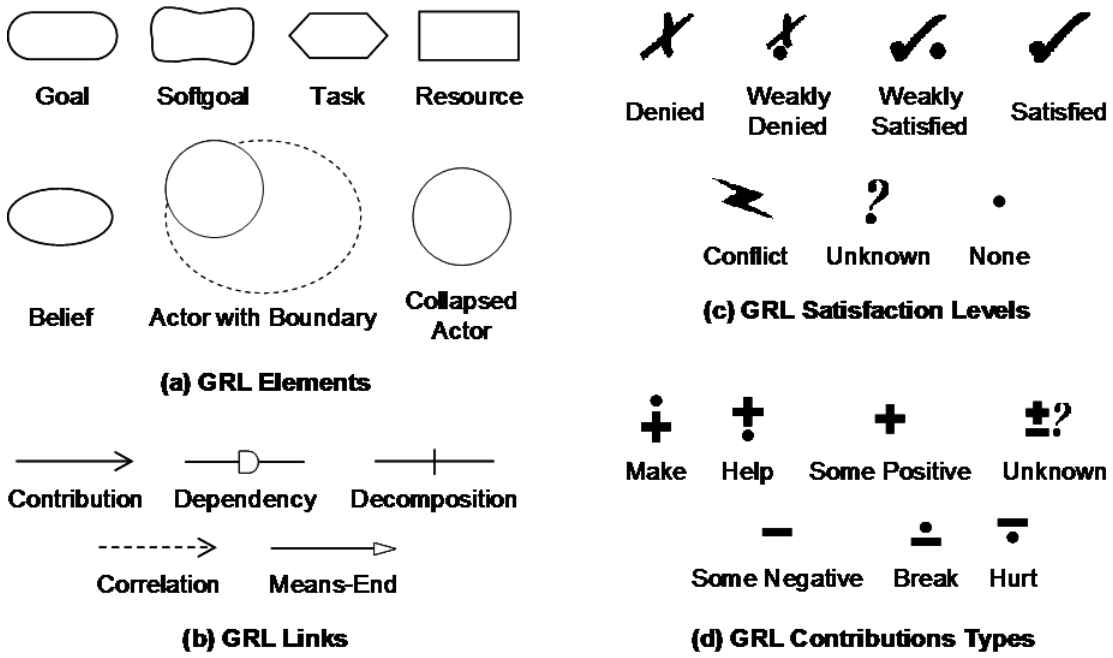

Figure 2.2: Basic Elements of the GRL Notation

2.4.2 GRL Evaluation Algorithms

A GRL model is evaluated by assigning initial satisfaction values to a subset of its intentional elements, and by propagating these values to the remaining intentional elements of the model through the links that connect them. Each collection of initial satisfaction values is called a GRL strategy. GRL models can be evaluated several times based on different strategies, mainly for comparison. Satisfaction values can be qualitative (Figure 2.2(d)), with a qualitativeVal attribute of type QualitativeLabel (*denied*, *weakly denied*, *weakly satisfied*, *satisfied*, *conflict*, *unknown*, *none*), or quantitative, with a quantitativeVal

attribute (an integer between −100 and 100). The satisfaction values capture contextual or future situations as well as choices among alternative means of reaching various goals. The quantitativeVal and qualitativeVal evaluation attributes of the intentional elements in the strategy are initially set to 0 and *none* respectively. These values are then propagated to other intentional elements via the links between them (i.e., contributions, decompositions and dependencies), according to algorithmic rules presented in this section. Note that these rules consider correlations in the same way as contributions.

To compute an actor's satisfaction level, an *importance* attribute (again quantitative or qualitative) may also be specified for intentional elements inside actors. This value defines the relative importance of an intentional element over the other intentional elements bound to that actor. The evaluation algorithm will make use of these importance values as well. The importance is shown between parentheses in intentional elements: (H)igh, (M)edium, (L)ow, or None for qualitative evaluations (importanceQualitative attribute), and an integer between 0 and 100 inclusively for quantitative evaluations (importanceQuantitative attribute). The values None and 0, which are the default values, are not displayed on diagrams.

Our GRL propagation algorithms, which are automated, allow the calculation of satisfaction values across multiple diagrams, can combine qualitative and quantitative contributions and satisfactions values in one model [16], and can resolve conflicts caused by contradictory contribution evidence. The satisfaction values can be also propagated to UCM elements linked to the GRL elements and through global integer variables.

GRL includes three general types of evaluations, formalized in three different algorithms:

- **Qualitative evaluation**: uses the qualitativeContribution attribute of contribution links, the importanceQualitative attribute of intentional elements, and the qualitativeVal attribute of intentional elements initialized from the selected evaluation strategy. This type of evaluation is appropriate in early requirements engineering phases, when specific quantitative data from the domain is difficult to acquire.

- **Quantitative evaluation**: uses the quantitativeContribution attribute of contribution links, the importanceQuantitative attribute of intentional elements, and the quantitativeVal attribute of intentional elements initialized from the selected evaluation strategy. This type of evaluation is more appropriate in late requirements engineering phases, when specific measures from the domain can be added to the model or when a finer granularity for these model parameters is required.

- **Hybrid evaluation**: uses any another combination of the above three categories of attributes (for contribution, importance, and intentional element evaluation values). This type of evaluation may be appropriate when only partial quantitative domain measures are available.

For all of three propagation algorithms, the satisfaction value for an intentional element is calculated in the following order: first decompositions, then contributions, and finally dependencies. These three algorithms all follow the same three basic steps:

1. Initialize the evaluation values of the GRL intentional elements based on the strategy selected;

2. Do a bottom-up propagation of the evaluation values to the other elements;

3. Calculate the satisfaction levels of actors.

The input of these algorithms is a GRL model and a selected strategy, and the output is a set of satisfaction values for each intentional element and actors in the model. The algorithms calculate the satisfaction values based on the order explained above. In the following subsections, we describe each of the algorithms in more detail.

2.4.3 A Quantitative Evaluation Algorithm for GRL

The quantitative evaluation algorithm uses *integer* values that range from -100 to 100 for the evaluation, and it uses the quantitativeContribution attribute of contribution links,

as well as the quantitativeVal attribute and the importanceQuantitative attribute of intentional elements. For each intentional element whose inputs are all known, the algorithm starts by calculating values for decomposition links, then contributions, and finally dependencies.

Calculating quantitative evaluations for decomposition links According to the type of decomposition (AND, OR, or XOR) of an intentional element, the satisfaction value is computed as follows:

- AND → the satisfaction value of the target intentional element is the minimum quantitative satisfaction values of all of its source elements.
- IOR (or simply OR) → the satisfaction value of the target intentional element is the maximum quantitative satisfaction values of all of its source elements.
- XOR → the satisfaction value of the target intentional element is the maximum quantitative satisfaction values of all of its source elements but with a warning if more than one source element has a quantitative evaluation value different from 0.

The result of this analysis is saved in an intermediate decompValue variable. An example of each of these decomposition types are shown in Figure 2.3. All of the source elements are initialized (*). (b) and (c) are different in that evaluating (c) generates a warning as more than one source has a value different from 0.

Calculating quantitative evaluations for contribution links For a target intentional element, the total quantitative contribution = $\sum$ (quantitative evaluation of each source element × its quantitative contribution level to the element).

In this algorithm (Figure 2.4), a predefined tolerance value is also given, which is used if there is no fully satisfied or denied contribution. With the help of the tolerance, many partial satisfaction or denial values do not add to full satisfaction or denial.

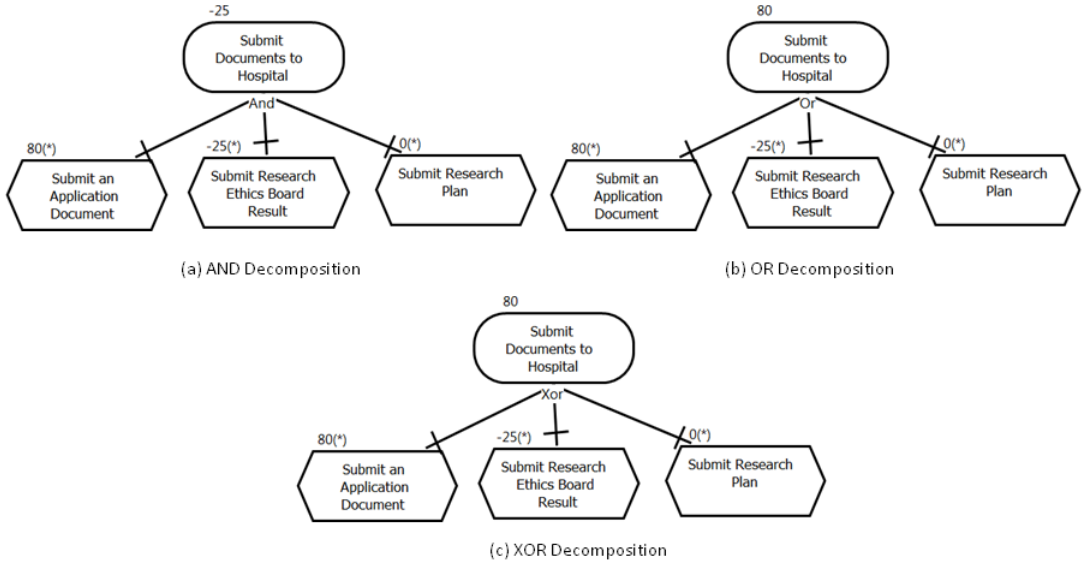

Figure 2.3: Quantitative Evaluation of Decomposition Links

The algorithm ensures that the satisfaction level of each intentional element will not go above 100 or below −100. Figure 2.5 shows an example of this algorithm with a tolerance value of 0.

Calculating quantitative evaluations for dependency links The dependency in this algorithm is calculated based on the following rule from the URN standard: *"The source element of the dependency links cannot have a satisfaction value higher than the target elements (which it depends on)"*. Therefore, the satisfaction value is the minimum between the contribValue returned from CalculateContributions and the satisfaction values of the dependee elements.

In Figure 2.6, the value for Patient PHI is initially 0 and the value of the goal Disclose Data to Researcher is initially −10. Since the value for Patient PHI is higher than the value for Disclose Data to Researcher, the value of Patient PHI changes to −10. However, the initial value of the goal Collect Statistical Data is calculated by the decomposition link as −25, which is less than −10. The value for Collect Statistical Data hence remains $min(min(-25, 0), -10) = -25$.

```
Algorithm CalculateContributions
Inputs element:IntentionalElement, decompValue:Integer
Output contribValue:Integer

tolerance:Integer        // predefined tolerance, between 0 and 49
oneCont:Integer          // one weighted contribution
totalCont:Integer = 0    // weighted sum of the contribution links
hasSatisfy:Boolean       // a weighted contribution of 100 is present
hasDeny:Boolean          // a weighted contribution of -100 is present
hasSatisfy = (decompValue == 100)
hasDeny = (decompValue == -100)

// compute the weighted sum of contributions
for each link:Contribution in element.linksDest
{
        oneCont = link.src.quantitativeVal × link.quantitativeContribution
        totalCont = totalCont + oneCont
        if (oneCont == 100) hasSatisfy = true
        if (oneCont == -100) hasDeny = true
}
totalCont = totalCont / 100
contribValue = totalCont + decompValue

// contribution value cannot be outside [-100..100]
if (|contribValue| > 100)
         contribValue = 100 × (contribValue/|contribValue|)

// take tolerance into account if a weighted contribution of 100 or -100 is not present
if ((contribValue ≥ 100 - tolerance) and not(hasSatisfy))
        if (totalCont > 0) // positive contribution
             contribValue = max (decompValue, 100 - tolerance)
             // else there is nothing to do, contribValue remains unchanged.
else if ((contribValue ≤ -100 + tolerance) and not(hasDeny))
        if (totalCont < 0) // negative contribution
             contribValue = min (decompValue, -100 + tolerance)
             // else there is nothing to do, contribValue remains unchanged.
return contribValue
```

Figure 2.4: CalculateContributions

Calculating quantitative evaluations for actors The quantitative satisfaction value for actor is computed as follows:

$$actor.quantitativeVal = \frac{\sum_{i=1}^{n}(elem_i.quantitativeVal \times elem_i.importanceQuantitative)}{\sum_{i=1}^{n} elem_i.importanceQuantitative} \tag{2.1}$$

where $elem_i$ is the ith intentional element bound to the actor.

In this algorithm, only intentional elements with an importanceQuantitaive value

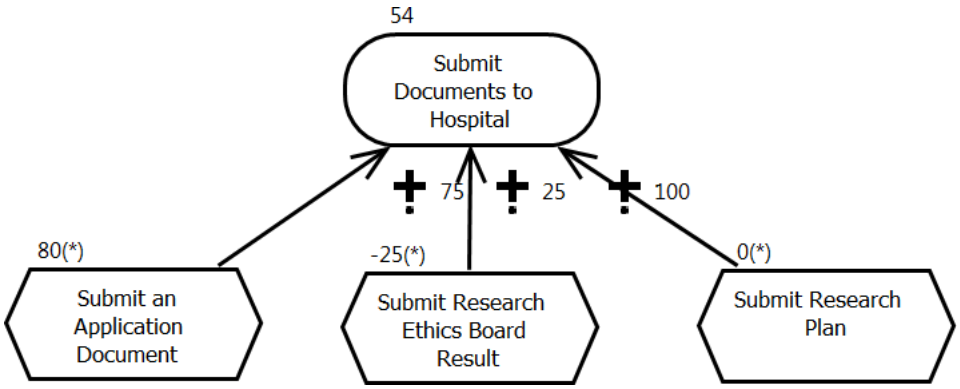

Figure 2.5: Quantitative Evaluation of Contribution Links

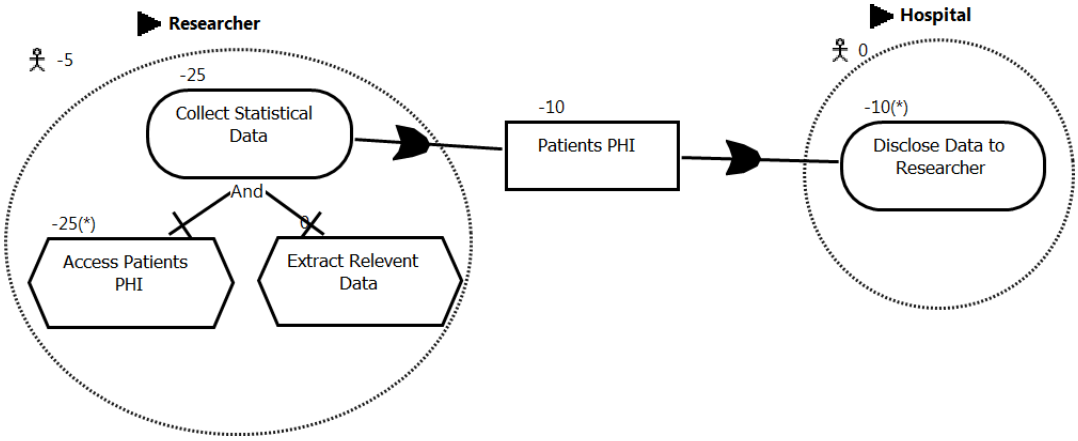

Figure 2.6: Quantitative Evaluation of Dependency Links

greater than 0 are counted. In Figure 2.7, the importance is calculated as follows: $((75 * 75) + (25 * 100) + (100 * 0) + (-25 * 25))/(75 + 100 + 0 + 25) = 37$.

2.4.4 A Qualitative Evaluation Algorithm for GRL

As previously explained, our qualitative GRL algorithm uses QualitativeLabel values for finding the satisfaction value of the target intentional element. As a result, the algorithm uses the qualitative contribution attribute of contribution links, and the qualitative importance (importance) and qualitativeVal attributes of intentional elements. The qualitative satisfaction labels, as discussed before, are *Satisfied*, *WeaklySatisfied*, *None*, *WeaklyDenied*, *Denied*, *Conflict* and *Undecided*. The qualitative values of the importance

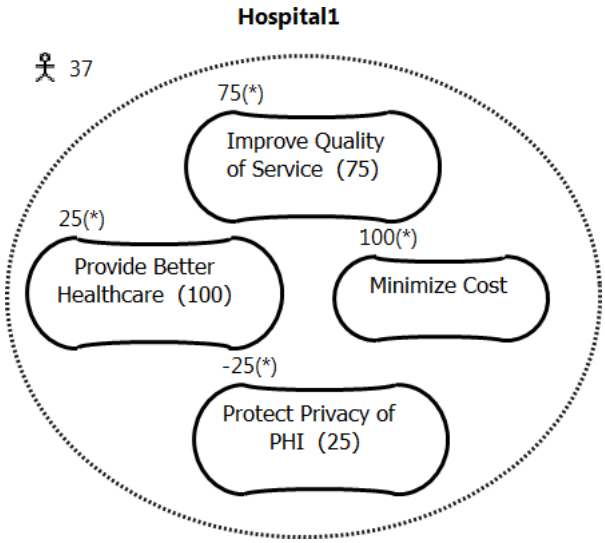

Figure 2.7: Quantitative Evaluation of Actor Satisfaction based on Importance Levels

factors are *High*, *Medium*, *Low* and *None*.

Since the qualitative values are discrete, the qualitative algorithm examines these values individually via a lookup table or a partial ordering.

Calculating qualitative evaluations for decomposition links According to the type of decomposition (AND, OR, or XOR) and similar to the quantitative algorithm, the satisfaction values are computed as follows:

1. AND → the satisfaction value of the target intentional element is the minimum satisfaction value of the source intentional elements in the order of $Denied < (Conflict = Undecided) < WeaklyDenied < None < WeaklySatisfied < Satisfied$.

2. OR/IOR → the satisfaction value of the target intentional element is the maximum satisfaction value of the source intentional elements in the order of $Denied < WeaklyDenied < None < WeaklySatisfied < (Conflict = Undecided) < Satisfied$.

3. XOR → the satisfaction value of the target intentional element is same as the one for IOR-type with a warning flag for the case where more than one source element have a quantitative evaluation value different from *None*.

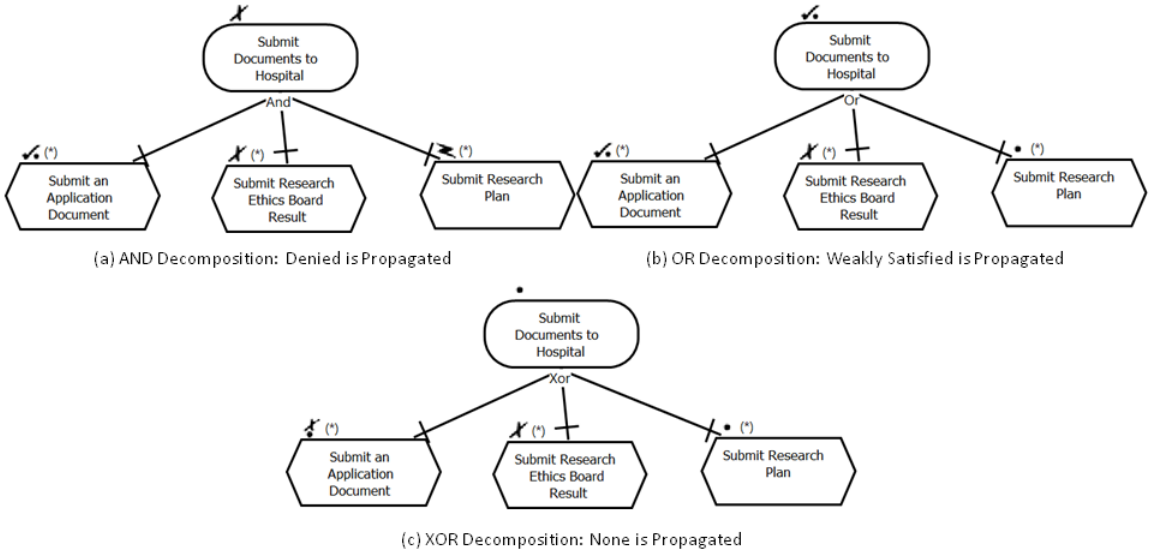

Figure 2.8: Qualitative Evaluation of Decomposition Links

In all of the three cases, *Conflict* results are substitute with *Undecided*. *Conflict* is not propagated to higher levels in the GRL model (which helps finding the root cause of the conflict).

Figure 2.8 provides examples for all three kinds of qualitative decompositions.

Calculating qualitative evaluations for contribution links To calculate the qualitative contribution, two algorithms are used. The main algorithm, CalculateQualitativeContributions (Figure 2.9), calculates the satisfaction value of the target with respect to a lookup table (Table 2.1) and returns *contribValue*. The other algorithm, AdjustContributionCounters (Figure 2.10), is used to increment the weighted contribution counters.

In Table 2.1, rows specify the possible qualitative evaluation values of the source, whereas columns specify the possible qualitative contribution types of the element's incoming contribution link. Note that previously found conflicts are not propagated by this function, which propagates *Undecided* instead.

The algorithm CalculateQualitativeContributions has three functions: CompareSatisfiedAndDenied (ns, nd), CompareWSandWD (nws, nwd) and CombineContributions (weightSD,

```
Algorithm CalculateQualitativeContributions
Inputs element:IntentionalElement, decompValue:QualitativeLabel
Output contribValue:QualitativeLabel

oneCont:QualitativeLabel          // one weighted contribution
ns:Integer = 0                    // number of Satisfied weighted contributions
nws:Integer = 0                   // number of WeaklySatisfied weighted contributions
nwd:Integer = 0                   // number of WeaklyDenied weighted contributions
nd:Integer = 0                    // number of Denied weighted contributions
nu:Integer = 0                    // number of Undecided weighted contributions
weightSD:QualitativeLabel         // partial weighted contribution from ns and nd
weightWSWD:QualitativeLabel       // partial weighted contribution from nws and nwd

// adjust the weighted contribution counters according to decompValue
AdjustContributionCounters(decompValue, ns, nws, nwd, nd, nu)

// compute the numbers of weighted contributions for each kind
for each link:Contribution in element.linksDest
{
        oneCont = WeightedContribution(link.src.qualitativeVal, link.contribution)
        AdjustContributionCounters(oneCont, ns, nws, nwd, nd, nu)
}

// check for the presence of undecided weighted contributions
if (nu > 0)
        contribValue = Undecided
else
{
        weightSD = CompareSatisfiedAndDenied (ns, nd)
        weightWSWD = CompareWSandWD (nws, nwd)
        contribValue = CombineContributions (weightSD, weightWSWD)
}

return contribValue
```

Figure 2.9: CalculateQualitativeContributions Algorithm

```
Algorithm AdjustContributionCounters
Inputs qualValue:QualitativeLabel
Modifies ns, nws, nwd, nd, nu:Integer

case qualValue of
        Satisfied:          ns++
        WeaklySatisfied:    nws++
        WeaklyDenied:       nwd++
        Denied:             nd++
        Undecided:          nu++
```

Figure 2.10: AdjustContributionCounters Algorithm

Table 2.1: Lookup Table for Computing Contribution Values (WeightedContribution)

	Make	**Help**	**Some+**	**Unknown**	**Some-**	**Hurt**	**Break**
Denied	D	WD	WD	N	WS	WS	S
WeaklyDenied	WD	WD	WD	N	WS	WS	WS
WeaklySatisfied	WS	WS	WS	N	WD	WD	WD
Satisfied	S	WS	WS	N	WD	WD	D
Conflict	U	U	U	U	U	U	U
Undecided	U	U	U	U	U	U	U
None	N	N	N	N	N	N	N

weightWSWD). The first two are used to find the value of the target node based on the number of *Satisfied-Denied* source nodes and *WeaklySatisfied-WeaklyDenied* source nodes. If there is at least one *Undecided* weighted contribution detected, then the result is *Undecided*, otherwise the three functions are computed consecutively.

In function CompareSatisfiedAndDenied (ns, nd), if all satisfaction levels are *Satisfied* without any *Denied* (i.e., ns $>$ 0 and nd $=$ 0), the return value is *Satisfied*. Similarly, if they are all *Denied* (nd $>$ 0 and ns $=$ 0), then the return value is *Denied*. If there are no *Satisfied* or *Denied* (ns $=$ 0 and nd $=$ 0), the result becomes *None*, whereas if both types are present (ns $>$ 0 and nd $>$ 0), then the result is *Conflict*.

In function CompareWSandWD (nws, nwd), if there are more *WeaklySatisfied* than *WeaklyDenied* (i.e., nws $>$ nwd), the returned value is *WeaklySatisfied*. If there are more *WeaklyDenied* than *WeaklySatisfied*, the functions returns *WeaklyDenied*. If the numbers are equal, it returns *None*.

Finally, function CombineContributions (weightSD, weightWSWD) calculates the final value of the source node. For this function, another lookup table (shown in Table 2.2), is used. In this table, the rows specify the possible qualitative values representing the global influence of weak contributions (i.e., weightWSWD), whereas the columns specify the possible qualitative values representing the global influence of *Satisfied* and *Denied* contributions (i.e., weightSD).

Figure 2.11 provides two examples with three contributions each. In (a), we have

Table 2.2: Lookup Table for Combined Contributions (CombineContributions)

	Denied	**Satisfied**	**Conflict**	**None**
WeaklyDenied	D	WS	C	WD
WeaklySatisfied	WD	S	C	WS
None	D	S	C	N

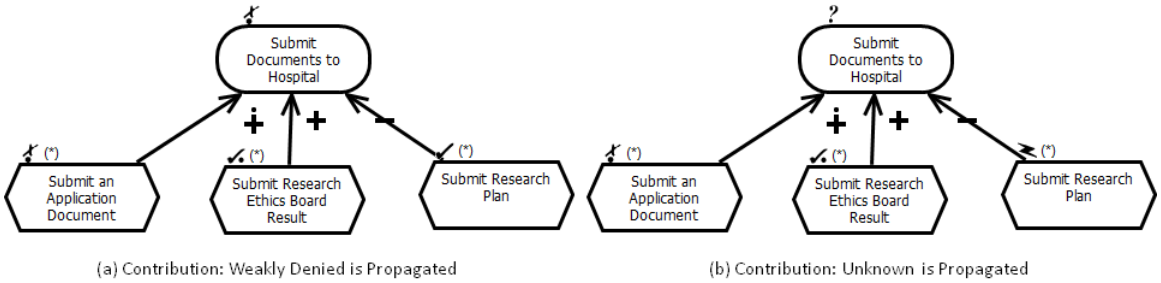

Figure 2.11: Qualitative Evaluation of Contribution Links

(WeaklyDenied and Make) = WeaklyDenied, (WeaklySatisfied and SomePositive) = WeaklySatisfied, and (Satisfied and SomeNegative) = WeaklyDenied. Comparing the numbers of *Satisfied* and *Denied* results in a 0:0 tie, and therefore we have a *None* value. The comparison of *WeaklySatisfied* and *WeaklyDenied* results in a 1:2 and therefore we get *WeaklyDenied*. Finally, the combined contribution of *None* and *WeaklyDenied* results in *WeaklyDenied*. In (b), we have (WeaklyDenied and Make) = WeaklyDenied, (WeaklySatisfied and SomePositive) = WeaklySatisfied, and (Conflict and SomeNegative) = Undecided. Since there is one *Undecided*, the result is *Undecided*.

Calculating qualitative evaluations for dependency links In a way similar to the quantitative calculation for dependencies, in the qualitative calculation the source element of the dependency links cannot have a higher value than those of the intentional elements it depends on (i.e., the target elements of the dependency links). As a result, the value of the intentional element will be the minimum value of the contribValue and the qualitative value of the target element. The order for the qualitative values is similar to AND-type decompositions: *Denied* < *(Conflict = Undecided)* < *WeaklyDenied* < *None* < *WeaklySatisfied* < *Satisfied*

Like for other qualitative calculations, *Conflict* is not propagated and it is substituted with *Undecided*.

Figure 2.12, illustrates an example of calculating qualitative satisfaction for dependency links. The value for Patient PHI is initially *None* and the value of the goal Disclose Data to Researcher is initially *WeaklyDenied*. Since the value for Patient PHI is higher than the value for Disclose Data to Researcher, the value of Patient PHI changes to *WeaklyDenied*. However, the initial value of the goal Collect Statistical Data is calculated using the decomposition links, and it evaluates to *Denied*. This value is less than the value of the target element (Patient PHI). Therefore, the value of the goal Collect Statistical Data remains the same.

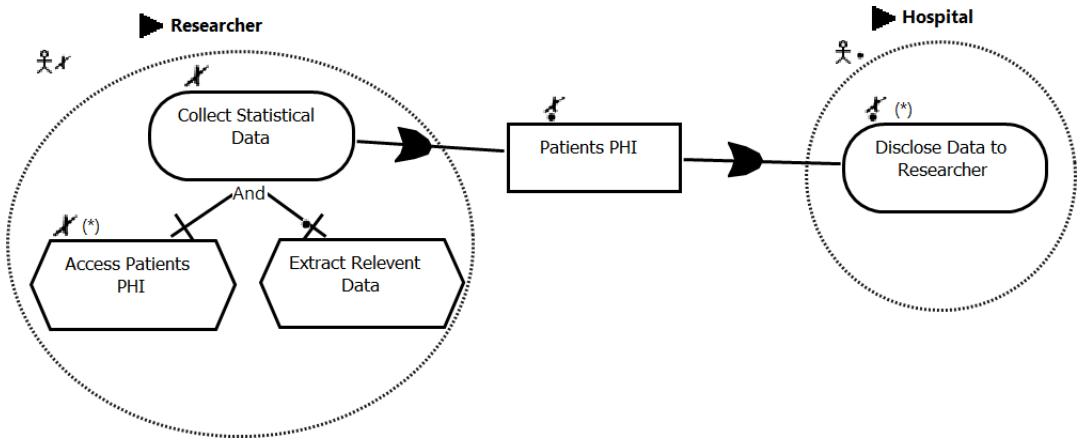

Figure 2.12: Qualitative Evaluation of Dependency Links

Calculating qualitative evaluations for actors In order to compute the qualitative evaluation value of an actor, the qualitative satisfaction value and qualitative importance value of each intentional element bound to the actor are used. The qualitative importance value of an actor is calculated in a way similar to the CalculateQualitativeContributions algorithm. The algorithm uses the WeightedImportance function, presented as a lookup table in Table 2.3.

Figure 2.13 presents an example for calculating the actor's satisfaction based on importance. The actor includes four softgoals, three of which with importance other

Table 2.3: Lookup Table for Weighted Importance

	D	**WD**	**WS**	**S**	**C**	**U**	**N**
High	D	WD	WS	S	C	U	N
Medium	WD	WD	WS	WS	C	U	N
Low	WD	N	N	WS	C	U	N
None	N	N	N	N	N	N	N

than None. The recalculated, qualitative evaluation values are:

- Improve Quality of Service: WeightedImportance (High, WeaklySatisfied) = WeaklySatisfied
- Provide Better Healthcare: WeightedImportance (High, WeaklySatisfied) = WeaklySatisfied
- Protect Privacy of PHI: WeightedImportance (Low, WeaklyDenied) = None
- Minimize Cost: WeightedImportance (None, Satisfied) = None

The comparison of the numbers of *Satisfied* and *Denied* results in a 0:0, and therefore the result is *None*. The comparison of the numbers of *WeaklySatisfied* and *WeaklyDenied* results in a 2:0, hence leading to *WeaklySatisfied*. Finally, the combined contribution of *None* and *WeaklySatisfied* results in an actor evaluation of *WeaklySatisfied*.

2.4.5 A Hybrid Evaluation Algorithm for GRL

This hybrid GRL algorithm uses integer values for the evaluation, and hence uses the importanceQuantitative attribute of actors and the quantitativeVal attribute of intentional elements initialized from the selected evaluation strategy. However, unlike the quantitative evaluation algorithm, the hybrid algorithm defined here uses the qualitative contribution attribute in contributions.

This is an example where quantitative and qualitative values are mixed. In this example, the discrete scale for contributions has 7 levels instead of 201 levels ($[-100..100]$)

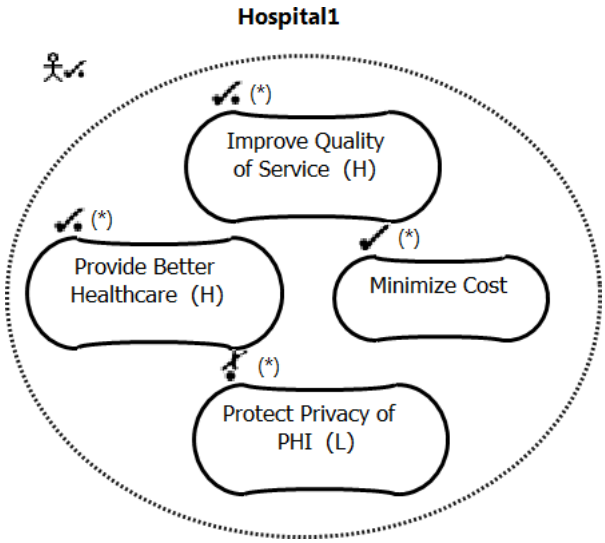

Figure 2.13: Qualitative Evaluation of Actor Satisfaction based on Importance Levels

as in the quantitative evaluation algorithm. This may improve the usability of models in domains where the weight of contributions cannot easily be determined with precision.

The algorithm first maps all qualitative contributions to quantitative contributions using Table 2.4. The content of this table reflects the relative ordering of qualitative contributions, however the associated quantitative numbers could be defined otherwise (e.g., 67 instead of 75, 33 instead of 25, etc.). When converting approximate qualitative labels to more precise measures, we run the risk of inserting a precision into our results that does not derive from an authoritative source, such as a concrete domain measure. It is important to keep in mind, when using hybrid methods, that the quantitative results are finer-grained approximations and not precise measures. Once all values are integers, the algorithm seen for the quantitative evaluation in Section 2.4.3 is used.

2.4.6 GRL Constraint-Oriented Semantic Evaluation Algorithm

The three algorithms mentioned in the previous sections are essentially bottom-up approaches. As such, these algorithms are only able to answer "what-if" questions. To eliminate this limitation, a generic and automatic algorithm based on a constraint-oriented

Table 2.4: Quantitative Contribution Values for Qualitative Contributions

Qualitative Contribution	**Quantitative Contribution**
Make	100
SomePositive	75
Help	25
Unknown	0
Hurt	−25
SomeNegative	−75
Break	−100

interpretation of goal models was recently introduced by Luo [70]. This algorithm aims to support bottom-up, top-down and inside-out analysis as well as optimizations in the presence of constraints.

In order to develop such algorithm, declarative mathematical semantics for GRL first need to be defined. Next, for such declarative semantics, a transformation is defined that targets a constraint-oriented language for which automated solvers exist. In the declarative semantics, syntactic constructs (i.e., intentional elements, decomposition, contribution and dependency links, actors and strategies) are mapped to evaluations via semantic functions.

Figure 2.14 illustrates four types of links considered in the constrained-oriented semantic evaluation algorithm. $v(S)$ represents the evaluation of intentional element S while CW_x represents contribution weights. For each link type, the evaluation is calculated as follows:

- AND-decomposition links: The satisfaction value of the parent S is the minimum satisfaction value of its children: $v(S) = min_{(1 \leq x \leq N)} v(A_x)$.
- OR- and XOR-decomposition links: The satisfaction value of the parent S is the maximum satisfaction value of its children: $v(S) = max_{(1 \leq x \leq N)} v(O_x)$.
- Contributions links: The satisfaction value of the target S is the weighted sum of the satisfaction values of its sources, bounded to ($[-100..100]$):
  $v(S) = max(-100, min(100, (\sum_{i=1}^{n} v(C_x) \times CW_x/100)))$.

- Dependencies links: The depender S cannot be more satisfied than its dependees: $\wedge_{i=1}^{n} v(S) \leq v(D_x)$.

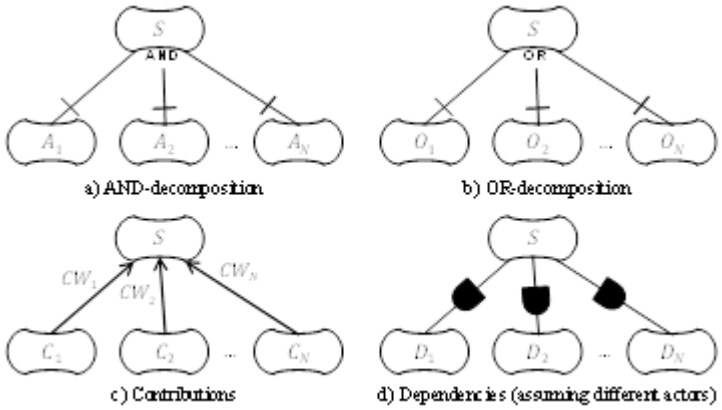

Figure 2.14: GRL Link Types

When the same intentional element has multiple types of links, the semantics is aligned with that of Section 2.4.3). This means that first decomposition values are considered, then contributions are added, and everything is constrained by dependencies.

Hence, for AND-decompositions, we get the following general relationship: $v(S) = max(-100, min(100, min_{(1 \leq x \leq N)} v(A_x) + \sum_{i=1}^{n} v(C_x) \times CW_x/100)) \wedge \wedge_{i=1}^{n} v(S) \leq v(D_x)$

The relationship for the OR-decomposition is similar, but with *max* instead of *min*.

This mapping to a constraint-oriented language leads to an algorithm that is more generic than the quantitative algorithm presented earlier. This algorithm can help answer "what-if" questions, but it can also find solutions to more interesting questions such as "is there a way to reach this satisfaction level for this top-level goal?", or more generically "what is the maximum satisfaction of this goal given these constraints on other goals?". However, the trade-off at this time is that tool support for Luo's algorithm is at a prototype stage, and not robust enough to replace the (robust) implementation of the quantitative, qualitative, and hybrid algorithms.

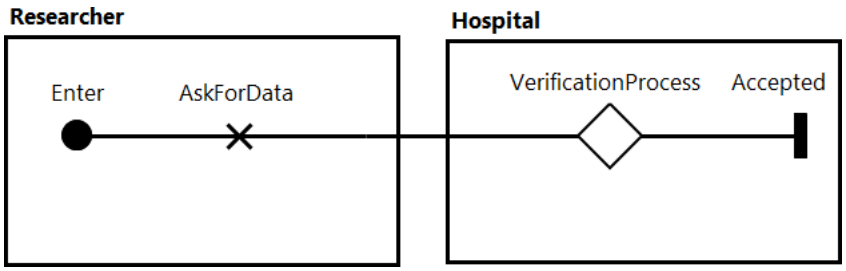

Figure 2.15: Use Case Map Example

2.4.7 Use Case Maps

The Use Case Map notation is used to model related scenarios and use cases in terms of causal sequences of responsibilities allocated to *components* (▭, e.g., Researcher in Figure 2.15). Components represent actors, roles, software modules, sub-systems, etc. and they can be decomposed recursively with sub-components. Scenario paths connect *start points* (●, e.g., Enter), which include preconditions and triggering events, to *end points* (▮, e.g., Accepted), which include post-conditions and resulting events. Paths contain *responsibilities* (✕, e.g., AskForData) which indicate where actions, activities, transformations, or processing is required. They can be performed in sequence, concurrently (⊣⊢), or as alternatives (⌒⌔).

Complex scenario maps can be decomposed using path elements called *stubs* (◇, e.g., VerificationProcess). Sub-maps in stubs are called plug-in maps. Stubs have identified input and output segments that can be connected to the start points and end points in the plug-in, hence ensuring scenario continuity across various levels of details. Dynamic stubs are used to specify alternative maps in the same location. Figure 2.16 recalls the basic elements of the UCM notation.

UCM support the definition of *scenarios* including pre- and postconditions. A scenario describes a specific path through the UCM model where only one alternative at any choice point is taken. UCM notation supports a simple but formal data model that can be used to formalize conditions at selection points (e.g., dynamic stubs and OR-forks). Responsibilities can also include code that modifies the values of the variables

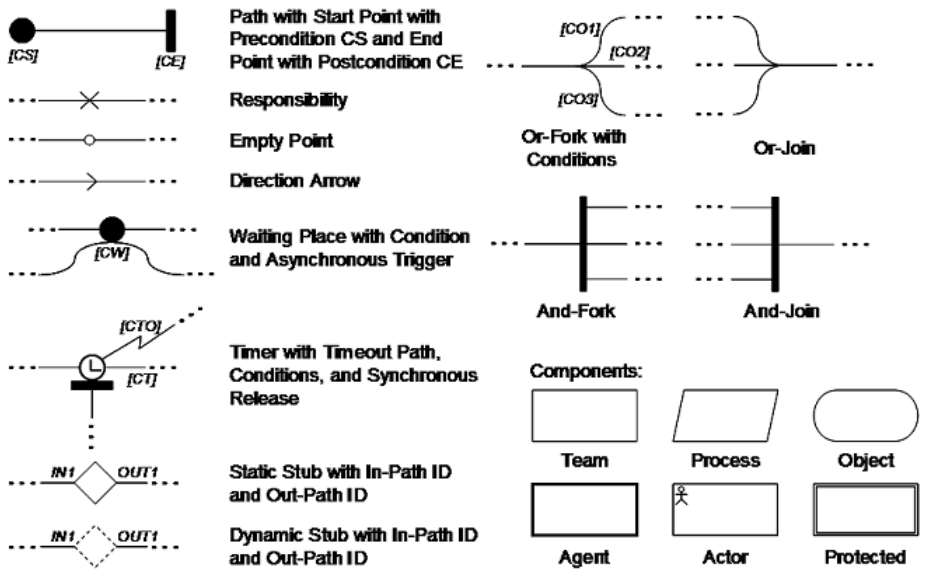

Figure 2.16: Basic Elements of the UCM Notation

used in this data model, including satisfaction levels of GRL intentional elements. A scenario definition is hence expressed with initial values for these variables, combined with a sequence of start points being triggered.

Given the definition of a scenario, a *path traversal mechanism* can simulate the scenario, and the traversed path can be highlighted or transformed to another representation (e.g., a message sequence chart diagram). The traversal mechanism essentially provides the operational semantics of the UCM language. It also turns the scenario definitions into a test suite for the UCM model, which is especially useful for regression testing as the model evolves.

2.4.8 Tool Support with jUCMNav

jUCMNav is an open-source Eclipse plug-in tool for URN modeling and analysis [80]. It supports modeling of both UCM and GRL as well as the *URN links* between them. It is possible to have a model with multiple views of the same model, which helps with scalability. The tool prevents the creation of syntactically incorrect URN models through

hard-coded rules, and more specific styles can be enforced through user-selectable semantic rules written in OCL. jUCMNav supports several GRL evaluation algorithms (including those explained in Sections 2.4.3 to 2.4.6), but only one UCM path traversal scenario mechanism (with a few parameters). It also allows exporting individual or complete models to different bitmap and report formats, importing/exporting reusable GRL catalogs, exporting the URN model to DXL format (for the IBM DOORS requirements management system), and exporting the results of GRL strategy evaluations in a comma-separated value (CSV) files.

2.5 Other Goal Modeling Notations

In this section, we give an overview of other popular goal modeling notations (i.e., *i**, Tropos, NFR, and KAOS) along with their analysis algorithms and tool support.

2.5.1 *i** Framework

Description

The *i** framework [115, 117, 116] supports the modeling of actors, their goals and their dependencies. It includes two types of models with different levels of abstraction. The *strategic dependency* (SD) model is used to model intentionality whereas the *strategic rationale* (SR) model is used to models rationales.

An SD model provides high-level overviews and includes a set of nodes that represent the actors (dependers/dependees) and a set of dependencies in terms of intentional elements that represent the relationships between them. Intentional elements can be goals or softgoals to be achieved, tasks to be done, resources to be provided/consumed, and beliefs. Actors as "dependers" can depend on other actors as "dependees" to satisfy an intentional element (the "dependum"). The dependencies between actors can have three different levels of importance, namely open, committed and critical. Furthermore, actors

in i^* are divided into four types: actors, agents, positions and roles. Actors, which are the supertype of the three other types, can perform an action. Roles are abstract characterization of the social behaviour of an actor in a specific domain. Agents are concrete actors such as humans or artificial hardware/software agents. Finally, positions are the roles assigned to an agent. Actors also have actor association links, which are classified into six types of associations:

1. Is-part-of (Part): Each group of actors can have subparts. The intentional dependency between the whole and its subparts are shown with is-part-of association.

2. Is-a: Represents the relationship between an actor and a specialized case of the actor.

3. Plays: Used to illustrate the relationship between an agent and a role. In this case, an agent *plays* a role.

4. Covers: Used to show the relationship between a position and the role it covers.

5. Occupies: Used to illustrate that an agent occupies a position.

6. INS: Used to represent an instance of an actor, an agent, a position or a role.

SR models, which provide lower levels of abstraction, are goal models that illustrate the intentional elements of an actor and the set of links between these intentional elements (thereby defining dependency refinements of SD models). Intentional elements in the SR model are connected to each other by contribution or correlation links. These links illustrate the negative or positive impact of the lower-level goals on the higher-level goals. Correlation links represent side-effects while contribution links document direct impacts. Alternatively, intentional elements can be decomposed by "means-end" links, which are akin to *OR links*, or "task-decomposition" links, which are *AND links*. Contribution or correlation links can have a qualitative satisfaction values among *make* (i.e., positive and sufficient), *some positive* (i.e., unknown positive), *help* (i.e., positive but insufficient),

hurt (i.e., negative but insufficient), *some negative* (i.e., unknown negative) and *break* (i.e., negative and sufficient). Means-end links model the contribution of some means (usually tasks) to the ends (goals, softgoals, tasks, and resources). Task-decomposition links are used to decompose tasks into some intentional elements.

*i** is a goal modeling approach that strongly influenced the TROPOS and GRL languages. Note also that Amyot et al. [3] have defined a profile for GRL that enables its use for supporting *i** modeling.

Evaluation Mechanism

One of the approaches for analyzing *i** models is a forward reasoning technique. Forward reasoning techniques start from the leaf of the goal model. In such technique, a qualitative value (i.e., satisficed, partially satisficed, conflict, unknown, partially denied or denied) is assigned to a set of leaf goals and these values are propagated to the high-level goals through the links. The other approach for analyzing an *i** model is backward reasoning. In such a technique, a desirable qualitative value is given to the target goal, the satisfaction values of the leaf nodes are calculated based on the target value and the links between the nodes [48]. Horkoff and Yu [49] recently provided an overview of several reasoning mechanisms for *i**, with en emphasis on interactive propagation mechanisms where the analyst solves detected conflicts.

2.5.2 TROPOS

Description

TROPOS [31] (a variant of *i**) is an agent-oriented software development methodology that includes the concepts of agents and goals. It supports four phases of software development:

- Early requirements analysis.
- Late requirements analysis.

- Architectural design.
- Detailed design.

In TROPOS, the software development process starts with defining stakeholders and their goals. The next step is to analyze, refine or decompose these goals into some other goals and to assign them to some actors until all goals have been assigned.

TROPOS focuses mainly on early requirements analysis rather than late requirements analysis. The first type of analysis deals with the organizational context of the system-to-be whereas the latter is concerned with functional and non-functional requirements.

In the early requirements analysis phase, TROPOS adopts *i** modeling concepts and diagrams. Namely, it defines Strategic Dependency models and Strategic Rationale models. However, in TROPOS, these models are called actor diagrams and rationale diagrams, respectively. Like SD models in *i**, actor diagrams include actors along with their interdependencies. An actor (depender) depends on another actor (dependee) for an intentional element (dependum). Similar to *i** and GRL, the intentional element can be a goal or a softgoal to be achieved, a task to be performed, or a resource to be used.

The TROPOS rationale diagram includes a set of goals, softgoals, tasks, beliefs and resources bound to a certain actor together with their *contribution* links and *AND/OR* links. The contributions have different strengths representing the level of satisfaction of a goal G and whether it contributes positively or negatively to the satisfaction of another goal. Contrary to *i** and GRL, in TROPOS there are only four (qualitative) contribution levels: -, --, +, ++.

Evaluation Mechanism

To model goals and to analyze the impact of different alternatives on high-level goals, TROPOS introduces the concept of goal graphs and axiomatization of goal relationships.

In goal graphs, the relationship between goals is identified as AND/OR relationships and +S, -S, +D, -D, ++S, --S, ++D, --D, +, -, ++, and -- contribution relationships.

S and D respectively mean *satisfiability* and *deniability*, and +/- mean the positive and negative propagation. For example, for AND/OR relationships, the meaning of the notations is:

(G1, G2,..., Gn) $\overset{and}{\rightarrow}$ *G: G is satisfied (or denied) if all Gi are satisfied (or at least one Gi is denied)*

(G1, G2,..., Gn) $\overset{or}{\rightarrow}$ *G: G is satisfied (or denied) if at least one Gi is satisfied (or all Gi are denied)*

In TROPOS, the goal relation in general is shown as (G1, G2,..., Gn) $\overset{r}{\rightarrow}$ G, for which the Gi are source goals, G is the destination goal of link r, and r is a relation or link between a source Gi and destination G node. AND and OR relations are called boolean relations, + and - relations are partial contribution relations and ++ and -- are full contribution relations.

Since contribution relations have different ranges, formal reasoning in goal graphs can become more complex. There are several factors that explain this complexity, including:

- Asymmetric value propagation, which means that achieving some goals may be only necessary but not sufficient to achieve another goal.
- Partial evidence, which means some source goals may only propagate a partial evidence about the satisfiability or deniability of the target goal.
- Conflicts occur when different goals contribute in contradiction to the other goals contributing to the same target goal.

The TROPOS goal modeling language supports both qualitative and quantitative relationships between goals and contains two types of analysis:

1. Forward reasoning.
2. Backward reasoning.

Before performing forward or backward reasoning, the goal relationship needs to be transformed into axioms. In this context, four predicates *FS(G)*, *PS(G)*, *FD(G)* and *PD(G)* are introduced. These predicates mean full or partial evidence that goal G

has been satisfied or denied. There is also another predicate, represented as $\top$, which implies that there is at least a "null" evidence that G is satisfied or denied. The order between these predicates is FS(G) $\geq$ PS(G) $\geq \top$. With these predicates and based on the ordering between them, several axioms can be deduced. Two invariant axioms are deduced directly from the predicates' ordering. They are FS(G)$\rightarrow$ PS(G) and FD(G)$\rightarrow$ PD(G) respectively. These axioms help propagate the satisfiability or deniability of the evidence in the goal graph. In addition, some combination of these predicates may lead to a weak conflict (if PS(G)$\wedge$ PD(G)), a medium conflict if (FS(G)$\wedge$PD(G)) or (PS(G)$\wedge$FD(G)) or a strong conflict (if FS(G)$\wedge$FD(G)). The axioms, together with the contributions, introduce some propagation rules that have been described in [31].

In qualitative forward reasoning, each leaf goal in the goal graph is assigned an initial value *(FS, FD, PS, PD)* propagated to other goals according to the rules specified in [31]. Based on different alternatives and their values, the higher-level goals and softgoals of a goal graph model can get different final values. Qualitative forward reasoning can also capture any conflict arising while satisfying a goal due to different initial values assigned to some goals.

In qualitative backward reasoning, the final values of some of the target goals have been given to figure out the possible initial value of some input goals. In backward reasoning, sometimes a cost value is assigned to the goal's satisfaction or deniability. Tropos uses the backward reasoning approach to analyze goal models and find a set of goals or alternatives that, if achieved, lead to the overall achievement of target goals and softgoals with minimum possible cost.

In addition to the qualitative propagation algorithm, a quantitative propagation algorithm is introduced in Tropos. In this context, two real constants *inf* (no evidence) and *sup* (full evidence) are defined. Different levels of partial evidence (w) are also considered between *inf* and *sup*. Two operators are defined as the evidence of satisfiability or deniability of the conjunction or disjunction ($\otimes$ or $\oplus$). Based on these operators and values, a probabilistic model is defined in which the evidence of satisfiability of G is given

as the probability that G is satisfied. With this probabilistic model and operators, new axioms and propagation rules can be defined.

2.5.3 NFR Framework

Description

The Non-Functional Requirements (NFR) framework [16, 81] is used to capture, model, and analyze non-functional requirements. The modeling approach in NFR is mainly top-down. NFR starts from a set of high-level non-functional requirements and then decomposes them until they achieve some operationalized requirements. With the help of the NFR evaluation mechanism, it is possible to analyze the impact of low-level alternatives on the high-level non-functional requirements in the model. Such analysis can help stakeholders to select the alternative that satisfies their needs and constraints better among several alternatives.

Softgoals, which are mostly qualitative and cannot be fully satisfied, are categorized into three groups: NFR, operationalizing, and claim softgoals. NFR softgoals are high-level non-functional requirements whereas operationalizing softgoals are low-level goals. The operationalizing goals are similar to goals and tasks in *i** and GRL, and they are used to satisfy the NFR softgoals. Finally, claim softgoals are used to capture rationales. Claim softgoals in NFR correspond to beliefs in *i** and GRL. These three types of softgoals are modeled in a Softgoal Independencies Graph (SIG) in NFR.

NFR has two types of links: contribution links and decomposition links. Contribution links illustrate the positive, negative, or unknown impact of a source goal on the destination goal. Negative impacts can be of type *Hurt*, *Break* or *Some-*, while positive impacts are one of *Make*, *Help* or *Some+*. The *Unknown* type is used when the impact of the goal on the other goal is not yet determined (but assumed to exist). Decomposition links are simple, conventional AND/OR links.

Evaluation Mechanism

The main NFR evaluation algorithm is a qualitative bottom-up approach. In this algorithm, the lowest level goals get satisfaction values that range from negative satisfaction (denied and weakly denied) to neutral (conflict and undecided) to positive satisfaction (weakly satisficed and satisficed). These values propagate to higher level goals through the contribution and decomposition links between them.

Users have to input the values for the lowest level goals. Since the conflicts have to be resolved by the users as well, the NFR propagation algorithm is semi-automatic. The algorithm works as follows: If there is a decomposition link of the type "AND", the lowest satisfaction value of all source nodes propagates to the higher level node. If the link is an "OR" decomposition, the destination node gets the highest satisfaction value among all of the source nodes. In contribution links, the satisfaction values adds up together with both the negative and positive value. When there are opposing evaluations of equal level of contribution to a target node, the algorithm propagates a "conflict" label to the target node.

2.5.4 KAOS

Description

KAOS [19] is a GORE method used to capture requirements in terms of objects, goals, actions, constraints, and agents. KAOS has a 3-layered framework for reasoning:

- a semi-formal layer for modeling goals,
- a qualitative layer for selecting between alternatives, and
- a formal layer for accurate reasoning [61].

In general, KAOS has a two-level structure; one for declaring concepts, their attributes and relationships with other concepts, and another one that is a formal level

for defining concepts. KAOS provides traceability links between its different layers to help refining the high-level goals into operational tasks, detecting conflicts, and assigning tasks to actors.

Goals in KAOS are categorized as functional (services) or non-functional (quality of services) goals. These goals are refined into other goals through "AND/OR" links until they are linked with the operations (actions) and are assigned to an agent. The KAOS methodology consists of the following steps:

1. Identifying goals of the system and decomposing them until we reach constraints and are able to assign them to agents (goal model).

2. Identifying objects and actions derived from a formal goal specification (object model).

3. Deriving object requirements and actions to satisfy the constraints.

4. Assigning objects, actions and constraints to agents (operation model) [19].

Evaluation Mechanism

KAOS uses a variation of the NFR evaluation mechanism (i.e., quantitative instead of qualitative evaluation) to analyze the impact of different non-functional requirements. KAOS uses quantitative data to evaluate partial satisfaction levels of goals and to find the impact of different alternatives on high-level goals. These quantitative values correspond to the qualitative values defined in NFR. In the KAOS evaluation algorithm, the degree of satisfaction for each high-level goal is the weighted average of the degrees of satisfaction of all its sub-goals [61]. Letier and van Lamsweerde [65] have also extended KAOS goal models with probabilities for reasoning about partial quantitative satisfaction in an automated way.

2.5.5 Tool Support for GORE

GRAIL

GRAIL, a tool that supports KAOS, combines a graphical view, a textual view, an abstract syntax view, and an object base view of a KAOS model. It helps in eliciting requirements, defining agents and the system's behavior, and linking these elements in a coherent model [6]. KAOS's declaration level is based on graphical and textual views whereas the KAOS definition level is handled only by a textual view. The tool includes the textual editor, the graphical editor, a syntax directed editor, a hypertext navigation, a LaTeX report generator, and an object base [19].

Objectiv*er*

Objectiv*er* is a commercial tool for goal modeling. This successor of GRAIL includes a KAOS model editor, a model browser, a model analyzer and a requirements document generator. The model editor supports multiple views of goals, objects, obstacles, agents and operations. It provides a diagram editor, a textual annotator, an explorer for hierarchical views and hypertext navigation. The model browser is used by stakeholders to validate models. It allows for navigation through models by checking diagrams and hyperlinks. The model analyzer is used to query the model to determine its completeness. It also provides supports to extract and visualize fragments of the model, and to generate use cases. Finally, the document generator is used to create requirements documents in RTF or PDF formats [60].

*i** Tools

The *i** goal modeling language is supported by several open source or research project tools, including OME, OpenOME, REDEPEND-REACT-BCN, TAOM4E, ST-TOOL and T-TOOL [41]. OME and OpenOME actually support *i**, NFR and GRL. OME is a Java standalone application and OpenOME integrates with other applications such

as Eclipse, Protege and Visio. The OME meta-framework supports objects such as nodes, links and expandable objects. REDEPEND-REACT-BCN supports modelling and analyzing *i** models especially in terms of information systems. TAOM4E supports the TROPOS methodology and it is used for model-driven software development. T-TOOL is used in the early requirements engineering phase and it provides a framework for formal analysis of requirements specifications. ST-TOOL is a graphical tool that allows modeling with the SecureTropos notation.

GR-Tool

GR-Tool is a graphical tool used for TROPOS to model goal graphs and perform forward and backward reasoning. GR-Tool also provides both quantitative and qualitative analysis for TROPOS. Complementary to GR-Tool, GOALSOLVE and GOALMINSOLVE are tools that have been implemented to support backward reasoning in TROPOS. Inputs to GOALSOLVE are the goal graph, a list of desired final values, a list of user constraints, and a list of goals that need to be considered as input goals. GOALMINSOLVE takes a set of weights for the goal values in addition to those mentioned above to support the minimum cost constraints.

2.5.6 Comparison Between GORE Methods

Among the modeling languages described above, TROPOS has the most complete set of goal model analysis algorithms. Like GRL, TROPOS includes both quantitative and qualitative evaluation algorithms and supports both bottom-up and top-down approaches. The tool support for TROPOS covers all of the different types of algorithms as well. NFR only provides qualitative analysis with a bottom-up approach. The qualitative algorithm is semi-automated as users define initial values. It propagates conflicts when the evaluation values of the source nodes are not of the same type and are contradictory. OME is a tool that supports the NFR algorithm. The *i** framework also includes a semi-automated, bottom-up qualitative approach, and more recently an interactive top-down qualitative

algorithm [49]. *i** has some tool support such as OME, the Eclipse-based *OpenOME*, and REDEPEND-REACT-BCN. KAOS only supports a quantitative version of the NFR qualitative algorithm. However, there is no tool for KAOS that supports the quantitative analysis algorithm, except a prototype mentioned in [65].

GRL includes bottom-up quantitative, qualitative and hybrid analysis algorithms, as well as a prototype constraint-based quantitative algorithm in jUCMNav. This tool also provides support for add new algorithms easily. GRL, contrarily to other goal modeling notations, is part of and international standard together with UCMs for business process modeling. GRL strategies are also an important part of that language. GRL also includes supports for profiling (through metadata, URL links, and even external OCL constraints) that allow it to be tailored for a particular domain (e.g., compliance) without the need to change URN or create a URN dialect. These capabilities are missing in the other goal modeling notations, yet they are essential for this thesis' compliance-oriented context.

Table 2.5 summarizes the comparison between the different GORE methodologies and GRL.

Table 2.5: Summary of Comparison between Goal Modeling Notations

	GRL	***i****	**Tropos**	**NFR**	**KAOS**
Modeling Language	Standard Language (ITU-T)	Not Standard	Not Standard	Not Standard	Not Standard
Analysis	Bottom-up Quantitative, Qualitative and Hybrid, Constraint Based Quantitative	Quantitative Bottom-up and Top-down	Bottom-up and Top-down Quantitative and Qualitative	Qualitative Bottom-up	Quantitative Bottom-up
Link with Business Processes	Combined with UCM	-	-	-	-
Strategy Definitions	Yes	-	-	-	-
Profiling Support	Yes	-	-	-	-
Tool Support	jUCMNav, OpenOME	OME, OpenOME, REDEPEND-REACT-BCN, TAOM4E, ST-TOOL and T-TOOL	ST-Tool, GR-Tool	OME, OpenOME	GRAIL, Objectiver

This being said, none of the current GORE tools specializes in the goal-oriented

analysis of business process compliance.

2.6 Nòmos Framework

The *Nòmos* framework is a goal-oriented modeling language that provides a methodology and concepts for requirements compliance problems. This framework includes three parts which are: (1) a language to model requirements and regulations, (2) an analysis method for checking the compliance and (3) a process to generate legally-compliant requirements in a systematic way.

In the *Nòmos* framework, legal statements are considered as well-formed sentences that are called normative propositions. Normative propositions (NP) consist of subject, object and legal modalities. The *Nòmos* framework is based on a Hohfeldian taxonomy of rights and it extends the i^* modeling notation.

The *Nòmos* meta-model represents predicates of a normative proposition and it contains two main classes: Actor and Right. Actor is the subject of the right. Right is composed of four sub-classes, namely: PrivilegeNoclaim, ClaimDuty, PowerLiability, ImmunityDisability. Each actor can have one or more rights while a right has exactly two actors (i.e., the *Holder* of the right and its *Counterparty*). In addition to these two main classes, in *Nòmos*, a proposition includes a prescribed action. Each right deals with one *PrescribedAction* modeled as the *Action* class. Also, a normative proposition may have priority over other normative propositions, which is shown through the concept of *Dominance* (Dominance Class).

In the *Nòmos* language, actors are shown as circles (similar to i^* notation). Actions are shown as triangles with links to both the Holder and the CounterParty actors. The four paired rights are distinguished as shown in Figure 2.17. In addition, the notion of *Dominance* is shown by the "$>$" symbol, which goes from the dominant action to the dominated one. A "realisation" relation is used to establish a relation between one element of the intentional model and one element of the legal model.

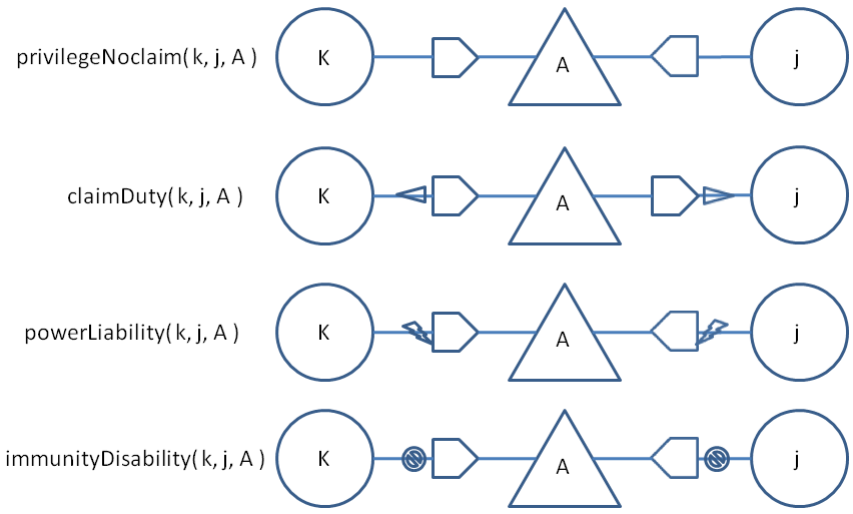

Figure 2.17: *Nòmos* Notation

2.7 Summary

In this chapter, we provided the background concepts and notations required for this thesis. At first, we defined what legal compliance for a business process is, and then we described regulations and some of the relevant taxonomies. We covered three taxonomies, namely the deontic logic, Hohfeldian, and Breaux taxonomies. We also clarified that we are adopting the first two taxonomies for our framework. We, then, gave an overview of the User Requirements Notation standard (GRL, UCM and tool support), with a particular emphasis on GRL and its current goal evaluation algorithms as our framework will build on them. For completeness, we also covered other existing goal modeling notations with their analysis techniques and tools as well as the current i^*-based legal framework called *Nòmos* framework.

The next chapter focuses on the literature related to requirements engineering and goal-oriented approaches to assess the legal compliance of business processes, and it will identify several opportunities for new contributions.

Chapter 3

Systematic Literature Review

As discussed in Chapter 1, organizations need to ensure and maintain their compliance with regulations. To help organizations be successful in this task, much work has been done in the scientific community. For example, some researchers apply requirements engineering approaches to ensure that business processes are compliant with regulations and policies while other researchers employ logic-based approaches for this matter.

In this chapter, we provide a systematic literature review of requirements engineering approaches for legal compliance of business processes with a special focus on *goal-oriented requirements frameworks*. A *systematic review* [68] is a rigorous methodology used to analyze all available publications in a particular research domain. In our review, we aim to explain scientific work and contributions made so far, which include goal-oriented requirements engineering methodologies for managing and maintaining business process compliance, while identifying gaps and what remains to be done.

For this purpose, we first define our methodology for performing this review. Then, we explain the results of our review, the contributions and the opportunities for improvement. Finally, we discuss the threats to validity and provide a summary.

Note that this review was produced in 2011 and then published in RELAW'11 [27]. The recent thesis work of Shamsaei [95] was incorporated afterwards.

3.1 Introduction

In the Requirements Engineering (RE) field, various literature surveys have been completed in the past, including three other systematic literature reviews in relation to legal compliance [83, 17, 96].

Otto et al. [83] examine 9 different areas for modeling regulations and monitoring compliance with policies and they explain the current contributions and the remaining problems in each category. Their research question is "what efforts have been made to model legal texts for use in requirements engineering and system development?". They selected 38 papers from the IEEE and ACM databases and categorized them in 9 groups: symbolic logic, knowledge representation, deontic logic, defeasible logic, first-order temporal logic, access control, mark-up based representation, goal modeling and reusable requirements catalogue. The work was successful in revealing some of the gaps and problems related to their research question. However, by limiting their search to only IEEE and ACM databases, there is the possibility that significant papers were missed that exist in other databases. Furthermore, their research question does not consider business process compliance or legal compliance frameworks in general.

Cleven et al. [17] examine regulatory compliance in information systems (IS). They select 26 IS-related papers from the IS journals provided by the London School of Economics. They also categorize papers into 9 categories and explain the contributions that have been made so far. Their focus is on information systems and, therefore, their categories are different from those in [83]. Their review does not cover any work related to compliance with goal-oriented requirements engineering methodologies. Moreover, by limiting their search to a single database (set of journals), there is the possibility of missing significant papers that exist in other databases. In our review, we go deeper into goal-oriented approaches for compliance management and try to ensure a more complete coverage by using the five databases in which requirements engineering papers are typically listed. In addition, we perform a manual search on highly relevant conferences,

workshops, and journals in requirements engineering to ensure the most significant papers are covered.

A recent and related systematic literature review in this field was conducted by Shamsaei et al. [96]. This review investigates the existing methods for compliance *measurement* based on either Key Performance Indicators (KPI) or goal-oriented modeling. In this work, 32 papers out of 198 papers were selected from four major search engines in computer science and they were categorized into five categories. For each category, the authors identified the major contributions and observable gaps. The main contributions identified are related to (i) compliance frameworks, reference models, and standards, to assess compliance, (ii) the measurement of compliance levels of processes based on KPIs and goal models, and (iii) the analysis of compliance with frameworks based on logic, URN or *i**. However, the authors mention that there is no work that combine goals with KPIs to measure the overall compliance level of an organization qualitatively and quantitatively. This literature survey mainly focuses on the measurements and KPIs for compliance and does not focus on the approaches related to extracting and modeling legal requirements, creating law-compliant business processes, prioritizing non-compliant instances and managing conflicts. In our review, we aim to address these issues and identify the contributions and gaps in each of the categories identified above.

3.2 Research Method

In our review, we follow the research method described by Loniewski et al. [68], itself based on Kitchenham's [58]. We divide the method into *three* high-level phases: planning the review, conducting the review and reporting the results.

Planning the review describes the process of selecting papers to review. In this phase, we identify: research goals and questions, keywords, sources, queries, inclusion/exclusion criteria, and classification criteria.

Conducting the review includes gathering the primary set of papers based on the queries identified in the previous phase from all of the sources, without filtering, and then filtering out irrelevant papers based on the inclusion/exclusion criteria according to the type (first layer), keywords (second layer) and abstracts and content (third layer).

Reporting the results involves:

- Categorizing and summarizing the final paper sets based on the classification criteria defined above;
- Identifying the contributions that have been made in each category; and
- Identifying the outstanding contributions for improvement and gaps with respect to research questions.

In the following subsections, we explain the first two phases while in Section 3.3 we describes the results.

3.2.1 Planning the Review

Here are the main steps followed to select the papers for the review.

Identifying Research Goals and Questions The objective of this literature review is to find publications that apply requirements engineering methodologies, and especially goal-oriented methodologies, for managing and maintaining business processes compliance. Accordingly, and based on the needs specified in Section 1, we define a primary question and a set of secondary sub-questions as follows:

What ***goal***-oriented ***frameworks*** are there that help organizations establish their ***legal compliance*** and manage the ***evolution*** of their compliance?

1. Are there any ***goal modeling*** notations that support ***modeling legal*** aspects and support ***compliance***?

2. Are there any methods or frameworks that can ***integrate legal requirements*** with ***business processes*** to provide law-compliant business processes?

3. Are there any guidelines for ***extracting legal requirements*** and ***mapping*** them to goal models?

4. Are there methods that provide ***templates*** for ***modeling compliant business processes***?

5. Are there ***methods*** that help organizations ***prioritize*** instances of ***non-compliance***?

6. Is there any ***tool support*** for managing compliance?

Identifying the Keywords With regards to the research questions, we select keywords that enable us to build our queries and select the relevant papers from the initial dataset: goal model, modeling or modelling, business process, legal compliance, compliant with law, law compliance, policy, regulation, legislation, requirement, and priority.

Identifying the Sources In our review, we conduct three types of searches. The first type is an automatic search using five core databases of scientific papers for requirements engineering: ACM Digital Library, IEEE *Xplore*, SpringerLink (SL), Scopus (SC), and Google Scholar (GS). The other two types of searches are manual searches to ensure the completeness and correctness of the automatic search. One of these searches is the manual checking of important conferences and journals in the area of requirements engineering with respect to law in the last 5 years (since 2006). We checked the Journal of Requirements Engineering (REJ), the International Conference on Advanced Information Systems Engineering (CAiSE), the Requirements Engineering conference (RE), the Requirements Engineering and Law workshop (RELAW), and the Workshop on Law Compliancy Issues in Organisational Systems and Strategies (iComply). Finally, the last search is meant to ensure that our review covers the related papers of researchers we

know to be working in this area, including the author of this thesis. It should be noted that our review did not follow up on the references found in the papers.

Identifying the Queries With respect to our primary and secondary questions, we defined an abstract query for the automatic search: ("goal" OR "requirements" OR "business process") AND ("modelling" OR "modeling") AND ("legal compliance" OR "law compliance" OR "compliant to law" OR "compliant with law" OR "compliance to legislation" OR "compliance to regulations" OR "compliance to policies"). We also defined another query for checking papers related to "priority", more specifically: ("legal compliance" OR "law compliance" OR "compliant to law" OR "compliant with law" OR "compliance to legislation" OR "compliance to regulations" OR "compliance to policies") AND ("Priority") AND ("goal" OR "requirements") AND ("modelling" OR "modeling").

These queries, though, had to be adapted to each search engine. For example, SpringerLink and Google Scholar cannot use a query that is longer than 64 characters. Therefore, we had to break the queries into two or more sub-queries for these two search engines. Other search engines, such as Scopus, do not accept parenthesis for single literals, however ACM needs parenthesis even for the single literals. Therefore, for each search engine, we customized the subqueries (not presented here) depending on the limitations of each search engine.

Identifying the Inclusion/Exclusion Criteria We defined three levels of exclusion for the papers. In the first level, papers are excluded based on their *type*. Any document that is a table of contents, an entire proceedings, a tutorial, a book, a standard definition, or not written in English, is removed from our set. In the second level, we check each paper for the keywords defined above. If the paper (in PDF) does not include ((goals OR requirements) OR (business processes)) AND (modelling OR modeling) AND (legal OR law OR policy OR standard) AND (compliance OR compliant), the paper is tagged *"No"* and is filtered out from our set. We do not include "priority" in our exclusion criteria, since there is not much work done for prioritization and there can be requirements engineering frameworks for legal compliance that do not consider priorities. However, if a paper has a "priority"

keyword in it, together with the above keywords, we include it in our dataset. The rest of the papers are tagged as *"Maybe"*, unless they are papers we are already familiar with, in which case they get tagged with *"Yes"*. In this stage, we also remove papers that are duplicates of papers identified by queries from other databases. These papers are tagged with *"Rep"*. Finally, in the last level of exclusion, we read the paper's abstract and content and filter out papers that are not related to goal-oriented/requirements engineering framework/methodology for managing and maintaining business process compliance (e.g., some papers on environmental management were removed here).

Identifying the Classification Criteria With respect to our research questions, we classify the papers into the following categories:

1. Requirements engineering framework for managing compliance. This category includes papers that describe compliance management frameworks based on requirements engineering notations (such as UML, URN, or BPMN) or logic-based approaches. These types of frameworks have to integrate legal documents, goal or requirements models, or business models into a single framework, provide traceability between different parts of the framework, and aim to establish, analyze, and maintain compliance for goal or business process models. They also have to provide a method for analyzing instances of non-compliance. (This corresponds to the *primary question*)

2. Goal modeling approach. This category regroups the papers that exploit or extend existing goal modeling notations or introduce new goal modeling notations to model legal requirements. (cf. *sub-question 1*)

3. Business process compliance. This group discusses papers that deal with compliance of business processes and that introduce methods to integrate legal requirements with business processes. (cf. *sub-question 2*)

4. Legal requirements extraction. This category describes papers that introduce guidelines for extracting legal aspects and/or their mapping to goal modeling notations. (cf. *sub-question 3*)

5. Law compliant business process templates. This group contains papers that provide templates for establishing compliant business processes. (cf. *sub-question 4*)

6. Legal requirements prioritization. This category includes papers that introduce methods for prioritizing legal requirements or non-compliant instances. (cf. *sub-question 5*)

7. Tool support. In this category, we cover papers that introduce tool support for managing compliance, as well as extracting and/or modeling legal requirements. (cf. *sub-question 6*)

8. Other legal compliance issues. This group covers papers that address legal compliance issues that do not fit into any of the previous categories, e.g., papers that compare different legal or privacy taxonomies, apply current methodologies to case studies, or focus on privacy in cloud computing or on using database approaches for privacy compliance. As papers in this category are less important for our objective, they will not be covered in detail in this review.

3.2.2 Conducting the Review

In this phase, we get the initial set of papers from the five source databases using our automated queries and then we perform manual searches to ensure completeness before filtering out irrelevant papers.

Building the Initial Dataset We gather all the candidate papers based on the search sources and queries described in the previous phase. In our work, we started with the ACM database (78 papers), followed by Scopus (86), SpringerLink (192), IEEE (190),

and Google Scholar (93) respectively. In our first manual search, we looked at two workshops (iComply (9 papers) and RELAW (27)), two main conferences (CAiSE (190) and RE (192)), and the REJ journal (93) between 2006 and 2011. We also made sure that we included the papers of the main researchers in this area. The relevant papers of these researchers (A. Siena, A. Antón, and E. Dubois) had already been covered by either the source engines or the manual search. This last step made us confident in the completeness of our dataset. Tables 3.1 and 3.2 summarize the numbers of papers (and their sources) considered for this study.

Table 3.1: Initial Search Engines Dataset

Queries	ACM	SC	SL	IEEE	GS	Total
Total	78	86	232	196	1135	1727

Table 3.2: Initial Manual Dataset

	iComply	RELAW	RE	CAiSE	REJ
Total	9	27	192	190	93

3.2.3 Filtering Irrelevant Papers based on Inclusion/Exclusion Criteria

After we build the initial data set, we need to decide whether the papers are relevant or not. As mentioned earlier, we perform this filtering in three steps which are explained as follows:

Type: In this step, from the set of papers that do not have a *"Rep"* tag, we remove papers that are tutorial, books, standard definitions, or not written in English from our set.

Keywords: Next, we search for keywords in the text of the remaining papers. We tag the papers with *"Yes"*, *"No"*, or *"Maybe"*, as discussed earlier.

Table 3.4 illustrates this step for a specific query on the ACM database. The first group of papers (first column) has most of the keywords, it contains "goal model" and

Table 3.3: First Iteration of Results Distribution

Search Engines	Yes	Maybe	No	Rep	Removed
ACM	4	9	11	47	7
SC	4	7	15	55	5
SL	7	18	70	137	0
IEEE	9	14	80	86	7
GS	3	38	176	660	258
Total	27	86	352	985	277

"business process", and it is known to us. This group is tagged as *"Yes"*. The second group of papers does not have "goal model" or "business process" as keywords, and has only the "model(l)ing" keyword; it is hence tagged as *"No"*. The third group of papers includes "business process", "model(l)ing" and "requirement" but it is not known to us. This group is tagged as *"Maybe"*. Table 3.3 shows the number of papers in each of the categories as determined by the classification criteria.

Table 3.4: Keywords

ACM Query			
Keywords	*1*	*2*	*3*
Goal Model	X	-	-
Business Process	-	-	X
Legal/Law/...	X	X	X
Compliance	X	X	X
Model(l)ing	X	X	X
Traceability	X	-	-
Evolution	-	-	-
Priority	-	-	-
Requirement	X	X	X

Abstracts and content: In the last step, we read the abstracts and content of the *"Maybe"* papers to change their tag to either *"Yes"* or *"No"*. The final numbers of papers selected from the search engines are shown in Table 3.5, whereas the numbers obtained from the manual search are shown in Table 3.6. The full list of papers selected is available in Appendix A.

Table 3.5: Final Results of Search Engines Dataset

	ACM	SC	SL	IEEE	GS	Total
Total	8	10	15	15	22	71

Table 3.6: Final Results of Manual Dataset

	iComply	Relaw	RE	CAiSE	REJ	Total
Total	4	7	2	2	2	17

3.3 Result of the Literature Review

Table 3.7 presents the total number of papers in each of the eight categories discussed in Section 3.2.1. It is important to mention that these categories are not mutually exclusive.

Table 3.7: Category Distribution

Source	Total	Proportion
RE Framework	16	15.1%
Goal Modeling	14	13.2%
BP Compliance	20	18.9%
Legal RE Extraction	15	14.2%
Law-compliant BP	2	1.9%
Prioritization	3	2.8%
Tool Support	12	11.3%
Others	24	22.4%

Here, we summarize the results of the most significant papers in each category, and then highlight important contributions and opportunities for improvement.

3.3.1 Most Significant Papers in Each Category

1) RE framework for managing compliance. In this category, many types of frameworks were identified. They differ in: i) visual notations, ii) guidelines used to develop the framework, iii) formal ontologies and iv) methods they use.

One important contribution in this category is the "compliance support framework" introduced by Hamou-Lhadj et al. [43]. This type of framework includes governance, people, process, and technology components. The governance component is used to ensure

compliance. It contains performance objectives, execution policies, internal management controls, and strategic alignment mechanisms. The process component provides an operational approach for delivering compliance. Finally, the technology component includes tools that are necessary for establishing, analyzing, and maintaining compliance. This framework does not provide a visual notation nor does it detail how to implement it. There is no formal ontology.

Breaux et al. [13] provide a distributed requirements management framework to ensure that regulatory obligations are integrated into functional software requirements. With this framework, obligations are satisfied either by refining them into functional requirements or by making new obligations delegated to others. This framework provides traceability between regulations, actor activities, and software requirements. The authors formalize the concepts of assignment, refinement, delegation, ownership, and decision sequence. Compliance analysis is based on certification (that business processes comply with regulations) or auditing (ensuring the continuation of the compliance). The authors also define requirements for tool support. This framework, in contrast to [43], provides more detail on how to establish and analyze the compliance. It uses grounded theory as a base for the framework and for extracting requirements. However, it does not provide a visual notation and it does not use any formal ontology.

In [105], Siena et al. introduce a framework and guidelines on how to generate legally compliant software requirements. The process described in the framework starts with *domain characterization*, which defines the relevant laws, followed by the development of a legal model based on a Hohfeldian taxonomy, and ends by refining this model into intentional elements and goal models for organizations. This process is unique in that it does not start with the development of a goal model. By starting with the legal model instead, the resulting goal model is expected to be compliant by construction. This work is still in an early stage. Unlike both previous approaches, this work provides a visual notation based on *i** and a formal ontology. However, it does not provide the means to integrate requirements unrelated to the law. There also is no mention of how to manage

evolution.

In [45, 44], Hassan and Logrippo aim to formalize privacy requirements with first order logic and provide a semi-automated compliance analysis method. A general mapping is provided from UML to a logical representation for enterprise and legal meta-models. For a specific organization, this mapping is used to obtain a Privacy Analysis Language (PAL) representation using the UML models available. The PAL model acts as input to a Privacy Analysis Tool (PAT), which is used to validate the requirements for compliance, consistency, and completeness. Similar to Siena's work, this work uses visual notations for representing models. It also uses a formal ontology for capturing enterprise definition. Although this approach helps identify cases of non-compliance, it has yet to define the patterns for transforming requirements to rules.

Maxwell et al. [74] use production rules to verify compliance of software requirements, and to identify new compliance requirements. Their approach has four steps whose inputs are production rule models [75] and requirements. In the first step, requirements terminology is mapped to the legal terminology of the production rule model. Requirements preconditions and legal preconditions are identified in the second and third steps, respectively. Finally, in the fourth step, query models are used to check the compliance. With the help of these rules, an analyst with little knowledge of the law is able to query the regulation model, find instances of non-compliance, and derive new legal requirements. This work, similar to Hamou-Lhadj's work and Breaux's, does not use any formal ontologies. However, in contrasts to all other work, this framework is based on a knowledge representation technique called "production rule". The framework does not provide a visual notation.

Another approach in this area is a requirements management framework for business process compliance, proposed by Ghanavati et al. [25, 26]. In this work, organizations and regulations are integrated into one single framework based on the User Requirements Notation [53] and they are connected through a set of traceability links. The framework has three layers. The top layer contains organizational process and policy documents as

well as regulation documents, the second layer includes the organizational and legal goal models, and the last layer contains business processes models for both organizations and laws. With the help of analysis algorithms (based on URN's) that leverage traceability links, it is possible to find instances of non-compliance and check the overall degree of compliance of the organization with the law. This work does not include guidelines on how to map legal statements to goal models. Like most of the work that has been presented so far, this also does not apply any formal ontology. However, similar to Siena et al., this work provides a visual notation (URN) based on *i** and on requirements engineering techniques.

Shamsaei et al. [95, 97, 98] introduce an Indicator-based Policy Compliance Framework (IPCF) that combines policy and rule models together with models capturing business goals, business process and their relative importance to the organization. This framework, which is based on the User Requirements Notation, helps to model the intent of the policies, goals and business processes. To evaluate and measure the compliance of the policies as well as identifying the non-compliant business processes, a set of indicators are used. The framework also contains a new GRL profile with a set of stereotypes specific to policies, OCL well-formedness rules, and an extended GRL analysis algorithm to model policies, identify conflicting situations and prioritize non-compliance instances based on the importance of the rules and the compliance level. This work modifies and extends the algorithms of Amyot et al. [2] and uses the same concepts as Ghanavati's work [25, 26]. However, it does not considers deontic modalities (like obligations and permissions) and does not handle multiple regulations.

2) Goal modeling approaches. In this category, we identified different goal modeling notations used to model legal requirements or build compliance frameworks. The majority of these papers apply *i**-based or Tropos-based notations such as *i**, *Nòmos*, SecureTropos, Secure *i** or GRL. In addition some of these approaches provide traceability between the legal goal model and organizational goal model (examples are [26, 52, 87, 103, 104]. However, one approach in this category uses Goal-Based Re-

quirements Analysis Method (GBRAM) method. The main contributions in this category are explained here.

Siena et al. [103, 104] introduce a new language based on *i** called *Nòmos*, which aims to bind the concepts of intentions or stakeholder's goals and regulations together. *Nòmos* models normative statements in terms of 8 classes of rights categorized into 4 correlative rights (i.e., duty-claim, privilege-no-claim, power-liability, immunity-disability). Each group has a subject of the right and a counterpart, and both are modeled with actors (which can have many rights). In addition, the framework includes activities that a right statement enforces. Legal requirements modeled with *Nòmos* are linked to organizational goals through a realization class. To establish compliance, the authors claim that the organization has to define goals to achieve the normative propositions modeled in *Nòmos*. The framework provides traceability between the legal model and the organization's goal model in the face of change, but the method for checking the compliance at each moment in time and finding instances of non-compliance is still manual.

In another approach to regulations modeling, Rifaut et al. [87] integrate *i** with the ISO/IEC 15540 standard to provide a formal framework to measure compliance of business processes with regulations. ISO/IEC 15540 defines a taxonomy for business process assurance goals. This taxonomy includes the concepts of *purpose* and *outcomes*. These outcomes can also be refined further with *indicators*. In Rifaut's work, each of these concepts is mapped to an *i** concept. For example, purposes are linked to softgoals in *i** model while outcomes are linked to goals. Indicators, which can be of type practices, work products and resources, are linked to tasks, resources and actors. The authors provide some support for traceability between the legal model and goal model but the compliance analysis is done manually. Furthermore, this framework is specifically focused on the ISO/IEC 15540 standard, and some regulations cannot easily be described with this taxonomy.

Ishikawa et al. [52] introduced an approach for managing legal interpretation with goal-oriented requirements engineering. In their work, legal interpretations are modeled

as high-level goals and then refined to more concrete goals. After modeling, they provide a gap analysis between the expected instances and the actual concepts. Finally these concepts are linked into a goal tree of the organization. Legal concepts are linked through *refined into* or *matched into* links to goals of the organization. The links between legal concepts and goals help to track changes. A gap analysis can help understand non-compliance instances. However, this work does not provide any tool support, so everything is done manually. The authors also do not use any official goal model and they do not explain the mapping between legal document and the legal model.

Ghanavati et al. [26] use and extend the Goal-oriented Requirements Language (GRL) to model legal documents and link such goal models to the goal models of organizations. With the help of these traceability links and the GRL quantitative and qualitative propagation algorithms, the authors analyze the degree of compliance of organizational goals against legal requirements and identify instances of non-compliance. However, this approach still does not include a guideline for mapping the legal statements to the intentional elements of a GRL model.

Breaux et al. [11] developed a semantic parametrization process to derive semantic models from goal models of policies built using GBRAM. GBRAM is an approach that helps identify system and organizational goals and refine them into requirements that can be achieved. The authors believe that goals are systematically and semantically difficult to analyze and compare, and hence they introduce a framework that helps represent rights, obligations, and permissions in a more formal way. Their framework has two parts: policy goal mining, which makes a goal model of policy documents, and semantic parametrization, which first transforms goals into restricted natural language statements (RLNS) and then parametrizes them to achieve semantic models. The semantic models help analyze conflicts, redundancies, and responsibilities with respect to queries in natural language. To parametrize the RNLS, three types of relations are used: the *root* relation that describes the main idea, *associative* relations, and *declarative* relations, which are between parameters and concepts. This work, unlike the approaches explained above,

does not provide any traceability between a legal model and an organizational model.

In [42], Halas et al. use SecureTropos to model and analyze organizational security requirements in the context of electronic archiving. They define organizational patterns for electronic archiving that are compliant with legal requirements, provide a solution to the problem, and model it with SecureTropos. However, determining whether legal requirements are integrated to the model, and how, is unclear. In addition, analysis and tool support are not discussed. Similar to Breaux et al., this work does not provide traceability between legal and organizational models.

Krausova et al. [59] propose to use legal patterns for building the trust relations in SI* (Secure *i**) models. Legal patterns are first written in natural language and then modeled with SI*. The structure of legal patterns is composed of the *legal context*, which entails organizational context integrated with some legal considerations together with the identification of the problem, *properties* of having compliance or certainty, and a *legal solution* that identifies ways to achieve compliance. Legal patterns are extracted either from the Directives enacted in European Union legislation or the science of legal theory. These patterns are mostly high-level so they can cover many cases. After defining the legal patterns in natural language, they are formalized with SI* and then the legal solutions are refined into new organizational structures annotated with legal requirements. To implement the legal solutions, it is necessary to know the partial activities that are done in the technical solutions. Therefore, legal patterns are described as business processes to integrate them. In this work, the mapping between legal patterns and SI*, as well as how to implement the patterns in terms of business processes, are not discussed.

3) Business process compliance. In this category, most papers focus on integrating business processes with legal requirements. Some of these approaches (such as [32] and [69]) apply deontic or defeasible logic while others do not have any formal methodology for this integration. Goedertie et al. [32] use a visual notation (the Business Process Model and Notation – BPMN) for modeling business processes whereas other approaches do not provide any specific notation. Kharbili et al. [57] and Lu et al. [69] try to use the

same notation for both business processes and laws. Kharbili et al. [57] use formal ontologies while the others do not use any formal ontology for business process compliance.

Karagiannis [54] provides a methodology to integrate regulatory compliance with business processes. The methodology uses a meta-modeling platform called ADOxx to integrate Business Process Management (BPM) and Enterprise Risk Management (ERM) meta-models into one single meta-model. The platform has 4 layers. The top layer is the meta-meta-model, with abstract classes, relationship definitions, and export/import functionalities. The second layer is the BPM-ERM meta-model, with a risk management library, working environment, document, and IT application meta-models. It is the base foundation for identifying potential risks and corresponding controls, and it serves as a connection between business processes and the risk-intensive part. The third layer contains the actual business processes models, risk management library, and working environment (i.e., the organization's structure). The last layer includes data about potential risks and their occurrences. The approach evaluates risks in linked business processes, and provides control processes resulting from risk management. Although integrating business processes with regulations is a good approach for managing business process compliance, the paper does not discuss how to extract risks and control objectives, nor how to manage traceability.

Lu et al. [69] present a method to provide compliance by building business processes with respect to legal requirements. The degree of compliance, defined with respect to a set of control objectives derived from legal requirements, can be non-ideal, sub-optimal, or ideal. Non-ideal means non-compliant, whereas sub-optimal means that although there are some violations, repairs are possible. To develop these compliant business processes, the authors start by formalizing them with logical terms and map them to compliance controls represented in FCL (Formal Contract Language), the combination of defeasible and deontic logics. Both business processes and control objectives are using the same logical notation. Then, the compliance is measured by checking whether the execution of sequences in the business process violates the rules in FCL. In addition, the

authors provide a quantitative measure for the degree of compliance, which ranges from 0 (non-compliant) to 1 (ideal). To find the degree of compliance, first for each control rule, a set of ideal and sub-optimal sequences are extracted and then the degree of support for these sequences in the process model is calculated. This work does not explain how to extract control objectives from regulations. There is no tool support mentioned in the paper and there is no method to prioritize the different rules. However, having a single logic notation for business processes and rules makes mapping and compliance checking easier.

In [57, 56], Kharbili et al. propose a framework for semantic policy-based compliance management for business processes. Their idea is to extend the business process ontology with a legal ontology, resulting in a compliance ontology. The framework starts with the policy document as an input and transforms it, using a structuring language, into structured policies. These policies are combined with generic policy, business rule, and business vocabulary ontologies through the semantic rules instanstiator. The result is a new ontology that includes a semantic model of policies as well as a logical representation of business rules. To analyze these models, the semantic policies are transformed into semantic operational rules and their compliance can be verified with an inference engine. This engine depends on the ontology language used to model policies, business rules, and business processes. This work is in its preliminary stage. Improvements are needed to define how the structuring algorithm and compliance checking algorithm can work, to explain how to integrate inference engine with this ontology, and finally how to provide tool support.

Schleicher et al. [94] present a refinement process for business process compliance based on a *compliance template*. The refinement layers introduced by the authors are compliance templates that are refined until they become executable business processes. Compliance templates include an abstract business process, a variability descriptor, and a compliance descriptor. The abstract business process defines how a business process is compliant. Variability descriptors provide a set of choices for converting the abstract

business process into executable ones. Compliance descriptors contain compliance links as well as compliance assurance rules. The refinement process starts from the abstract process of a compliance template and continues by fulfilling the constraints of that layer with a set of activities. Finally, these activities are validated against the constraints and the same process continues by moving up to another layer, where the constraints are propagated. When the constraints from other layers add to the higher layer, they can cause conflicts that can be modeled in classic logic to determine whether they are satisfiable. When the constraint region is filled with activities and whenever a constraint is satisfied, it will be deleted from the set. This helps avoid some of the potential conflicts. This work also provides tool support that extends the web-based BPMN editor Oryx with features needed for the refinement layer process.

In [32], Goedertie et al. create regulatory business processes with the help of temporal deontic assignments. These business processes are intended to be used only for verification and not for execution. The authors use the PENELOPE language, which includes obligation, conditional commitment, and permission modalities. These three concepts help differentiate between possibilities and necessities in business processes. To develop regulatory business processes, a state space composed of deontic assignments is generated with PENELOPE and then these assignments are mapped to control-flow processes, defining a set of activities to perform. To make the flow, a business interaction can go from one state to another only if there exists a set of permissible performances between these two states. The generation of these business processes is automated with an algorithm implemented in Prolog. For modeling business process, the authors use BPMN. Generating compliant business processes automatically is very helpful, but this work assumes that a set of obligations and permission statements exist to guide this generation.

4) Legal requirements extraction. In this category, several methods for extracting legal requirements from legal documents have been identified. Some have formal ontologies for the extraction (such as Siena et al. [104]) while the others (such as Breaux [11]

and Maxwell and Antón [75]) do not include any formal ontology. Furthermore, different authors use different techniques for this extraction. For example, Siena et al. apply requirements engineering techniques, Breaux et al. use grounded theory, Maxwell and Antón apply knowledge representation methods, and Hassan and Logrippo [46] use first-order logic.

Breaux et al. [11] use Semantic Parametrization to extract rights and obligations from regulations and to clarify their potential ambiguities. They developed a systematic approach for generating a formal legal model by eliciting legal requirements in terms of permissions, obligations, and constraints from legal texts [14]. Their work illustrates that legal documents are very complex, vague, and described at an abstract level.

In [75], Maxwell et al. explain how to generate production rules from legal texts. Production rules are used to build an if-statement rule-based repository. The first step for developing production rules is the *raw translation* of legal text into Prolog and then *rule refactoring* to eliminate duplicates and group conditions. The raw translation includes five sub-steps. First, rules are classified according to their type: rights, permissions, or obligations. Second, one identifies parameters of each rule, which are actors, their counterparties, and the source of the rule. Next, one identifies the preconditions for the first rule, and then all the disjunctions from rules have to be removed and new separate rules have to be built. Finally, the *implied* obligations, permissions, and rights are identified. Refactoring the produced rules is done in several ways: 1) by grouping cases (if the rules are only different in cases, a new predicate is introduced that entails all of the cases and reduce the number of rules to one), 2) by grouping common conditions (all rules that have a same condition are grouped as one), and 3) by reinforcing implied rules with the actual rules (i.e., by merging both rules in one rule that covers both). The final result of these steps is a production rule model that is used to check requirements compliance.

Young et al. [113, 114] provide a commitment analysis methodology that helps operationalize requirements from commitments, privileges, and rights. The method has four

steps: parsing policy documents into individual statements, classifying policy statements, documenting statements based on a defined template, and operationalizing statements into requirements. The statements are classified based on scope, actors, and concepts. The scope can be either procedural or legal, actors are organizations and users, and concepts are of the types commitment, privilege, right, or unclassified. To decide the type of the concept, the authors use modal verbs. Based on the 2 options for scope, 2 for actors and 3 for concepts, there can be 12 different classifications. With regards to the type of classification, they derive a set of requirements from that statement.

In [46], Hassan and Logrippo explain how a UML class model called Government Extraction Model (GEM) can help to extract legal requirements from plain legal text. GEM provides a semi-formal representation of entities and their relations, but it does not automate the extraction process. The authors classify the legal statements into three meta-types, namely procedural, declarative and ontology statements. Procedural statements are of the type *if-then* whereas declarative statements declare facts or system properties that need to be refined into procedural statements. Ontology statements can be either organizational structure statements or process ontology statements. Furthermore, legal requirements can be statements of type Access-Right (AR), Delegation of Authority Right (DOR) or Separation of Concern (SOC). AR statements can be implemented as procedural statements, while DOR are specific types of AR statements and as a result can also be procedural. SOC statements can be either declarative or procedural. The classes in GEM are activity, user, legal entity, role, and process (atomic or composite), which are used to identify ontology statements. Procedural statements show the role name of the association links between the classes. Based on these classes and their roles, the modeler classifies each statement and extracts and refines the legal requirements. This method still lacks guidelines as it is not clear how legal requirements are created. This work does not include mechanisms for traceability. Also, there is no link between different parts of the law to trace the hierarchy of statements inside a single law.

Siena et al. [102, 103, 104] introduce a meta-model that contains four correlative classes of rights. Legal statements are formalized as duty-claim, privilege-noclaim, power-liability, or immunity-disability classes. The object of a right (action), the subject of a right (actor), and their counterparts are also derived from legal documents. The relationships between the formalized legal statements are provided through priorities among them. For example, a power statement can override a duty. In their other works, these authors present a visual notation for law modeling and discuss how to achieve compliance with requirements.

5) Law-compliant business process templates. In [29], Ghanavati et al. describe the steps needed to build a framework that integrates law modeling notations with business process modeling notations. With the help of law-compliant strategic goal models and different types of legal statements, they try to provide a set of templates for business processes. Their framework has 4 layers that connect abstract high-level legal actions to concrete operationalized tasks through the concept of purpose. In the third layer, the *Nòmos* framework [103] is used to model legal statements (fourth layer). The User Requirements Notation is used to model goals (second layer) and business processes (first layer). This work is very preliminary and without an implementation.

Note that the "compliance templates" in [94] are actually a framework that helps refine business processes to achieve and validate compliance. This is different from this category's templates, which focus on high-level business processes derived from law itself. Those templates can be used as a base for organizations to start building their own business processes.

6) Legal requirements prioritization. There is little work done on how to prioritize requirements in order to address compliance issues. Massey et al. [72, 71] discuss a prioritization methodology that involves a numerical priority assignment for legal documents. This approach calculates a prioritization scale, which is the sum of four metrics computed from mappings of requirements to legal documents, subsections contained in legal documents, exceptions, and references. Requirements are then categorized into

two groups: ready to implement or in need of more elaboration and investigation. This grouping is based on the score each requirement gets during the prioritization effort. Although this approach helps identify requirements in each group, it does not consider the level of importance of the legal requirements from an organizational point of view.

Siena et al. [104] also use the concept of *dominance*, which shows the priority of source rights to the target and the priority of one type of legal statement to others. However, this method also does not consider organizational goals and the negative impact of non-compliance instances on organizations while prioritizing legal requirements.

7) Tool support. In [45], Hassan and Logrippo implemented a Privacy Analyzer Tool (PAT) to validate enterprise requirements against legal requirements. This tool is used to find violations and to determine whether the enterprise model is consistent with legal requirements. PAT can load enterprise and legal documents that are described in PAL. PAT converts the specification to the *Alloy* language and then uses the Alloy Analyzer tool to analyze the model with respect to different themes.

The Web-based Privacy Goal Management Tool (PGMT) [11] is used to model policies as goals. PGMT contains more than 1200 goal statements extracted from over 100 Internet privacy policy documents. In PGMT, goals are documented in a format starting with a specific keyword followed by a verb that explains the action an actor has to perform. After documenting goals in this format, goals are classified according to the subject and then refined to remove redundancies and inconsistencies.

jUCMNav [80] is an Eclipse-based URN tool that supports modeling goals and business processes with GRL and UCM. It also has automated GRL qualitative and quantitative evaluation algorithms to help analyze goal satisfaction. In recent years, a light-weight profile has been added to this tool to enable the integration of legal models with goal models and the detection of instances of non-compliance.

There is very little tool support for modeling legal requirements in terms of goals, logic, or business processes. However, some such as [45] and [80] integrate modeling, analysis, and compliance verification features into one single tool. Still, none of these

tools provide links between the actual legal documents and legal requirements extracted from them. These links need to be handled separately, e.g., via external requirements management tools [25].

3.3.2 Contributions Made in Each Category

Many contributions have been made in the past decade. Requirements engineering frameworks have been developed that aim to establish compliance in organizations. Most have some kind of traceability links between business processes, goal models, and the original regulations to be able to manage any potential changes. Some of these frameworks provide automated, semi-automated, or manual analysis (either with the help of goal modeling analysis algorithms or logic) to find instances of non-compliance. Furthermore, goal modeling notations and their extensions have been used in many approaches to model regulations in terms of goals, tasks, actors, and their interactions. Many researchers address the integration of legal requirements with business processes. Some build legal business processes automatically from regulations or use the same notation for both business processes and laws. In addition, significant work focuses on extracting legal requirements from regulation documents. These legal statements are finally modeled using modalities such as obligations, permissions, commitments, constraints, or with duty, claim, privilege, no-claim, etc. At times, extracted legal statements are also linked to goal or business process models. However, very little work has been done to prioritize legal requirements and to make templates for law-compliant business process. Tool support is limited to a few examples such as PAT, PGMT, and jUCMNav, which help analyze and manage compliance.

3.3.3 Opportunities for Improvement

Even with significant contributions in this field, there are still some research problems that deserve more attention:

1) Business process compliance framework. It is necessary to have a concrete framework with guidelines on how to extract legal requirements, how to map them to business processes and how to analyze the compliance.

2) Methodology for prioritizing legal requirements. It is necessary to consider that legal requirements do not all have the same impact on organizational objectives. Furthermore, not all non-compliance instances have the same importance with respect to the law. Ensuring compliant business processes is a time-consuming and expensive activity for organizations. Therefore, it is critical for them to be able to prioritize tasks related to compliance.

3) Templates to create law-compliant business processes. Regulations are usually vague and hard to understand, especially for software engineers. It is necessary to provide templates or samples to help organizations build compliant processes more easily.

4) Improved linking between legal requirements and business processes. Although there are some frameworks that put all the right elements together, there is still a gap between extracted legal requirements and business processes, especially in terms of impacts.

5) Improved goal modeling notations and analysis. Goal modeling notations were not initially meant to model legal elements. Also, most goal-based analysis algorithms are currently bottom-up. Yet, it is necessary to extend the goal modeling notations to cover all legal aspects and perhaps even enable one to perform top-down analysis (i.e., find how to satisfy specific goals).

3.4 Threats to Validity

In our literature review, we strived to get the most complete and correct set of scientific publications. We selected four important search engines in computer science, combined with Google Scholar in order to get papers that have been published in other journals

or libraries. In addition, we manually searched the most important journal, conferences, and workshops related to Requirements Engineering and Law. Furthermore, we made sure that papers of well-known people in this field have been covered by our search. We defined an abstract query that covered our research questions' keywords to be able to get a maximum number of publications. We also used exploited synonyms and homonyms of the keywords in the queries.

However, we did not include theses, books, tutorials, standards, and non-English publications. Moreover, we did not check the references included in the papers, although we believe our 3-layer paper extraction covers most of the related references. Also, in searching for the keywords, it is possible that we missed important synonyms. In the second step for selecting the relevant papers, we did a manual search on papers based on their keywords and counted the number of times each keyword was repeated in the paper. If this number was less than 3, we assumed that the paper was not relevant (and this might be too restrictive).

Finally, this systematic literature survey was performed in 2011, and more recent work has not been systematically incorporated (except for the work of Shamsaei, which is close to ours).

3.5 Summary

In this chapter, we provided a systematic literature review of goal-oriented frameworks for business process compliance against laws and policies. We selected 88 papers from a list obtained from five search engines and five additional conferences, journal, and workshops. We categorized these papers into eight groups addressing our research questions and provided a summary of the most significant papers in each category (except the category *"Others"*). This study allowed us to identify five important research areas that deserve further attention (Section 3.3.3). The next chapter will describe a new model-based method for managing legal compliance of business processes that will pro-

vide contributions towards addressing four of these five areas (numbers 1, 2, 4 and 5 in Section 3.3.3).

Chapter 4

LEGAL-URN Framework for Developing Legally Compliant Business Processes

In this chapter, we describe the LEGAL-URN framework for achieving business process compliance. This framework provides models and tool support for:

1. gathering legal constraints, business processes and organizational goals,
2. providing means to identify instances of non-compliance, and
3. prioritizing these instances.

In presenting our framework, we first define the problem (Section 4.1) and the potential solutions (Section 4.2). Then, we provide an overview of our LEGAL-URN framework (Section 4.3), its components (Section 4.4), the framework meta-model (Section 4.5) and the steps needed to use it (Section 4.6). In Section 4.7, we describe each layer of the framework in detail as well as different types of links. Next, we formalize and implement the framework as a URN profile in Section 4.8. Finally in Section 4.9, we define our method for analyzing compliance based on the framework.

4.1 Problem Definition

In Chapter 1, we stated that organizations need to be compliant with regulations while still satisfying their own strategic goals. We also discussed the complexity of regulations and the need for a systematic approach to help organizations manage and maintain compliance. In Chapter 3, we explored the literature and analyzed the gap between the state of the art and what is actually required. We identified the following set of problems that need to be addressed in this context:

1. There are no specific guidelines on how to model legal statements with existing goal modeling notations.
2. Existing goal modeling notations cannot capture all aspects of legal statements.
3. Goal modeling analysis algorithms are mostly bottom-up and there is no analysis algorithm specific to legal compliance.
4. There is neither a systematic way to analyze the compliance of business processes to the law nor a method to manage this compliance.
5. There is no methodology available to prioritize non-compliance issues.
6. There is no template-based method for building law-compliant business processes.
7. Business processes and law models are not appropriately linked with each other.
8. Guidelines to integrate several laws in one model and resolve conflicts are currently lacking.

This thesis tackles these problems (except item 6) and provides suitable solutions.

4.2 Potential Solution

To solve the problems stated in the previous section, we propose our LEGAL-URN framework that leverages requirements engineering models and tool support to:

1. Model legal documents in the same notation as used for organizational models.
2. Integrate both organizational and legal models in one framework with appropriate links between them.
3. Extend the current GRL modeling notation to capture legal modalities.
4. Identify mapping rules between modalities in legal texts and the eight Hohfeldian classes of rights.
5. Identify rules for modeling legal statements with goal models.
6. Maintain compliance when business processes or legal documents evolve.
7. Measure the compliance of organizational procedures quantitatively and qualitatively.
8. Identify and prioritize instances of non-compliance.
9. Integrate all necessary regulations in one model and resolve their potential conflicts.

This chapter covers items 1 to 5, items 7 and 8 are addressed in Chapter 5, and item 9 is addressed in Chapter 7. Item 6 is a property inherited from previous work of Ghanavati [24, 25], which exploits a commercial Requirements Management System (IBM DOORS) to manage such changes in URN-based models. as this solution is reusable as is, it will not be explored further in this thesis.

4.3 LEGAL-URN Framework Overview

In [23], we introduced a three-layer requirements management framework for compliance. That framework did not address all of the problems mentioned in Section 4.1, although it provided partial solutions for items 1, 2, and 4 in Section 4.2. As illustrated in Figure 4.1, this old framework is subdivided into three layers and two parts. On the right-hand

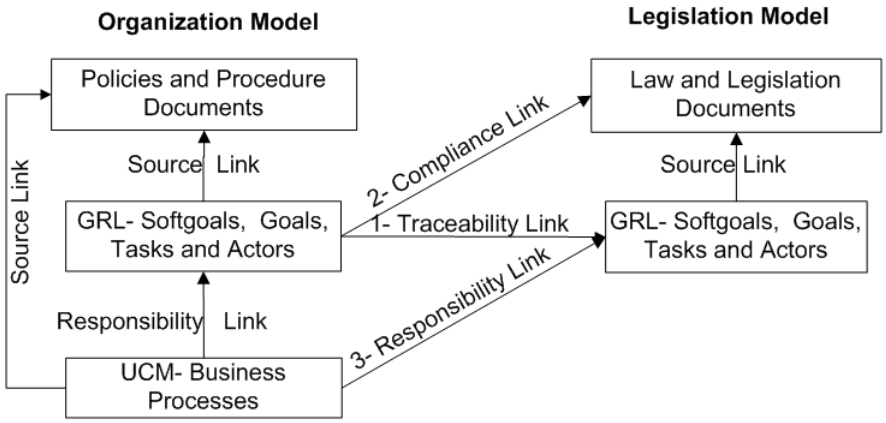

Figure 4.1: Old Requirements Management Framework for Compliance (2007) [23]

side of the framework illustration, there are legal models and legal documents alongside a legal goal model, while on the left-hand side, the organizational models including their corresponding organizational policy documents are displayed, together with the organizational goals and business processes models. In order to manage compliance, a set of traceability links between the models is provided. We are able to identify missing elements via an inspection of the missing links. Change is managed by tracing the links. These links are static and have no degree of impact (i.e., they are simply present or not). To analyze compliance, it is necessary to export the models into an external tool (IBM/Telelogic DOORS) and create links between them there. Furthermore, in that framework, legal goals are of the same type as organizational goals and there is no clear distinction between obligation goals and permission goals in the legal model. As a result, there is no clear guideline on how to extract legal goals from legal documents [25, 24].

In this thesis, we now introduce a new model-based framework called **Legal-URN** that has four layers (shown in Figure 4.2) and that can address the problems identified in Section 4. In this figure, the dotted lines represent the differences between this framework and the old framework (Figure 4.1). The Legal-URN framework contains the following features (Figure 4.3):

- 4 distinct layers for documents, Hohfeldian model, goal model, and business process

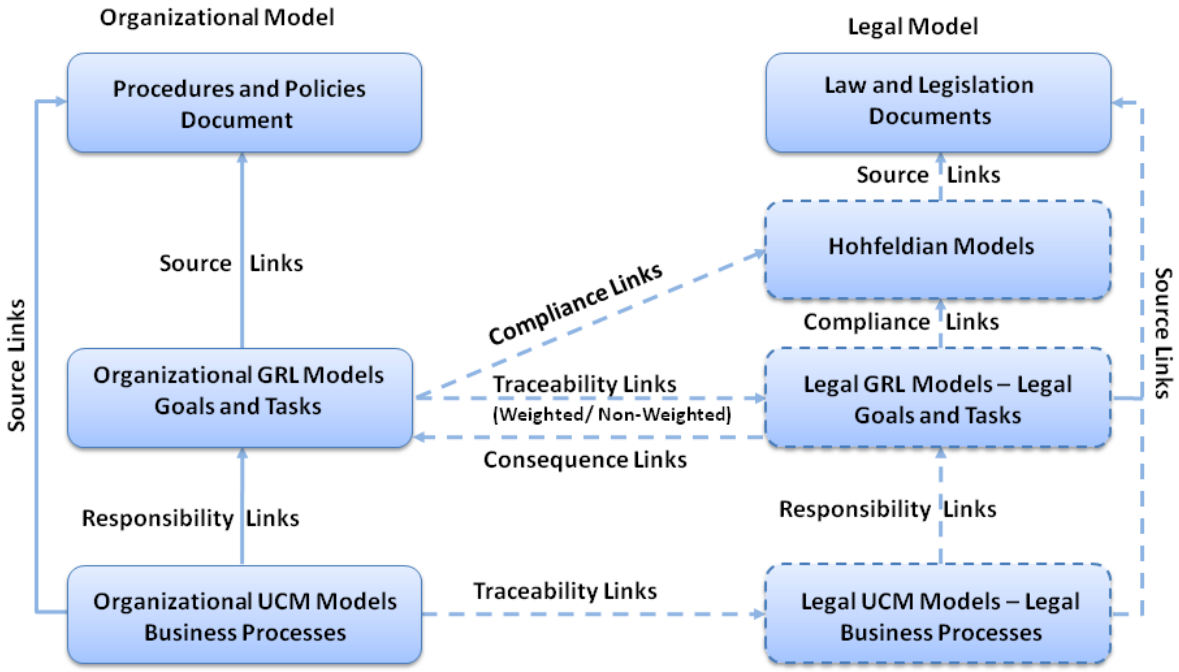

Figure 4.2: LEGAL-URN Framework Overview

model.

- Different links (weighted, simple and new types).
- Hohfeldian classification of rights applied to the model of legal goals.
- OCL rules for checking the well-formedness of the models.
- Legal profile in URN that helps to distinguish legal goals from organizational goals and that contains consequence goals to capture the effect of non-compliance instances on organizations.
- New compliance analysis algorithms that leverage the new Hohfeldian classification concepts.
- New prioritization algorithms to help prioritize which instances of non-compliance to address first.

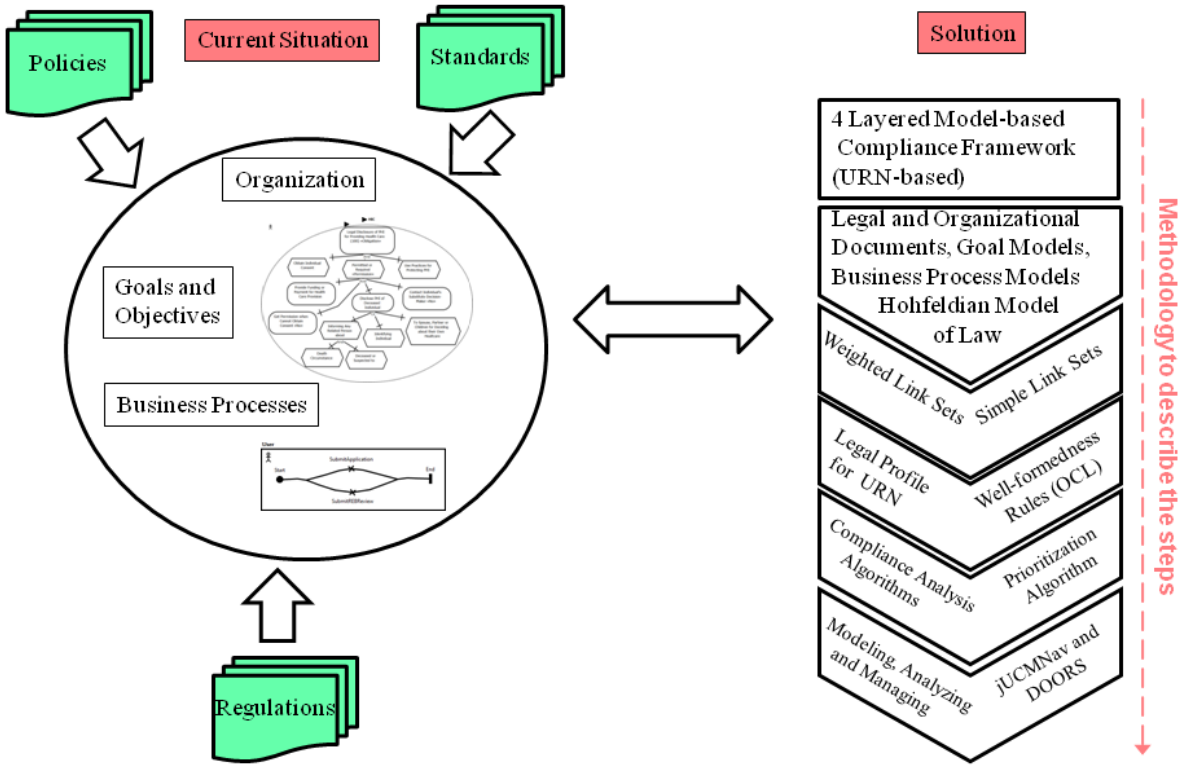

Figure 4.3: Current Situation and Proposed Solution

- Methodology that describes the steps to develop the models and links, as well as steps to analyze and maintain compliance.
- Tool support for modeling, analyzing and managing compliance.
- Methodology to handle more than one law and resolve conflicts or overlapping cases.

4.4 LEGAL-URN Framework Components

The four layers of our LEGAL-URN compliance analysis framework (shown in Figure 4.2) are:

1. Official source documents that define the legislation on one side and organizational structures, policies and processes on the other side.

2. Hohfeldian model of the law which consists of a set of Hohfeldian statements (*Nòmos* [105] could also be adopted, as explained in Section 2.6).

3. Goal models, using URN's Goal-oriented Requirement Language, which capture the objectives and requirements of both the organization and the legislation.

4. Business process models, using URN's Use Case Maps, which define the business processes that implement organizational policies as well as representing steps mandated by legislation.

To be able to connect the different pieces of the framework together, we introduce 5 types of links between the 4 layers of the framework and legal and organizational parts:

1. **Source links** map the goal, Hohfeldian, and business process models of the law and of the organization back to their source documents.

2. **Compliance links** map directly from legal and organizational goal models to the Hohfeldian model of law.

3. **Traceability links** map the correspondence between organizational models and legal models (at the goal model level and at the business process model level). Traceability links are divided into *simple* traceability links and *weighted* traceability links.

4. **Responsibility links** document which business processes implement or are responsible for which parts of the goal model.

5. **Consequence links** demonstrate the impact as it applies from legal goal models to the organizational goal models.

4.5 Legal-URN Framework Meta-Model

The framework meta-model shown in Figure 4.4 formalizes the concepts of the legal and organizational models, as well as their relationships. The meta-model contains two parts: the top part shown in *green* is for the legal model and the bottom part shown in *blue* is for the organizational model.

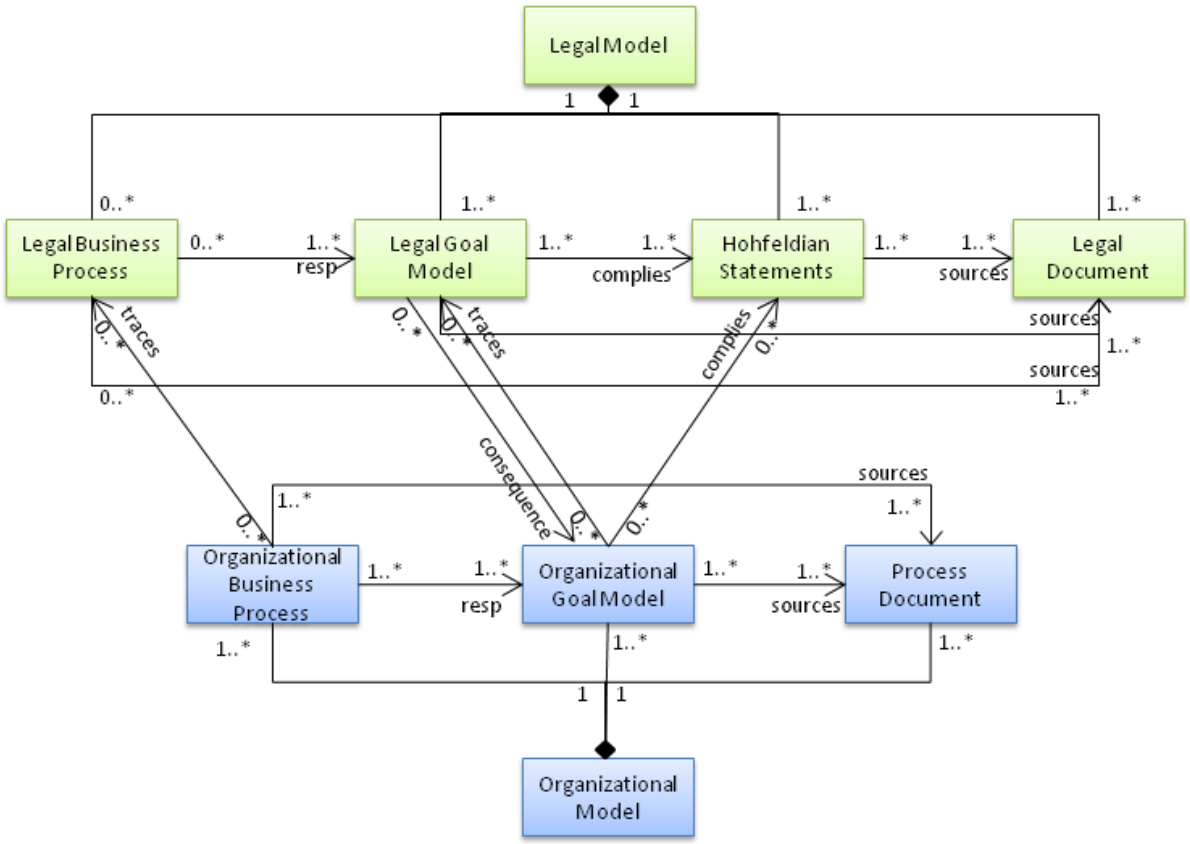

Figure 4.4: Legal-URN Framework Meta-model

Each legal model contains 1 to many legal documents, 1 to many Hohfeldian models, 1 to many legal goal models and 0 to many legal business process models. Legal documents are mapped to the Hohfeldian models, legal goal models and legal business processes through source links. Each Hohfeldian model can have 1 to many relationships to legal goal models, and each legal goal model can represent 1 to many Hohfeldian models. The

links between them are tagged as "complies". Legal business process models only exist for procedural legal documents, therefore there can be 0 to many such models in the legal model. When present, legal business process models are linked to the legal goal models through responsibility links showed with "resp".

The organizational model has 3 parts: 1 to many process documents, 1 to many organizational goal models and 1 to many organizational business process models. Organizational goal and business process models are linked to the process documents through source links. Similar to the legal model, the links between organizational goal model and business process model are of "resp" types.

Links of types "traces", "resp", "complies" and "consequence" describe respectively traceability, responsibility, compliance and consequence links between legal and organizational models.

4.6 Steps for Using the LEGAL-URN Framework

To use the LEGAL-URN framework in a given context, the following steps need to be taken (see also Figure 4.5):

- **Step 1.** Identify relevant legal and organizational documents.
- **Step 2.** Developing a Hohfeldian model of law - Classify each statement of the legal document based on Hohfeld's classes of rights (refer to Section 2.2.2), while linking them to the source legal document (via source links).
- **Step 3.** Refining Hohfeldian model of law - Refine the *Power-Liability* and *Immunity-Disability* statements of the Hohfeldian model into multiple *Duty-Claim* or *Privilege-NoClaim* statements.
- **Step 4.** Developing Legal GRL - Develop the goal model of the law and annotate the intentional elements with «Permission», «Obligation», «Precondition»,

«Exception», and «XRef» tags. Create source links to the legal documents, and compliance links to the Hohfeldian model.

- **Step 5.** Developing Legal UCM - Develop the business process model of law if necessary and link it to the goal model. Create source links to the legal documents, and responsibility links to the goal model.

- **Step 6.** Developing Organizational GRL and UCM - Develop the goal model and the business process model of the organizations. Create source links to the organization's procedure and policy documents, as well as responsibility links from the business process model to the goal model.

- **Step 7.** Defining Consequence Goals and Model - Identify the «Consequence» goals as the consequence of non-compliance.

- **Step 8.** Establishing Framework Links - Establish the links (compliance, traceability, and consequence) between the legal and organizational models.

At this point, the models are ready to be analyzed.

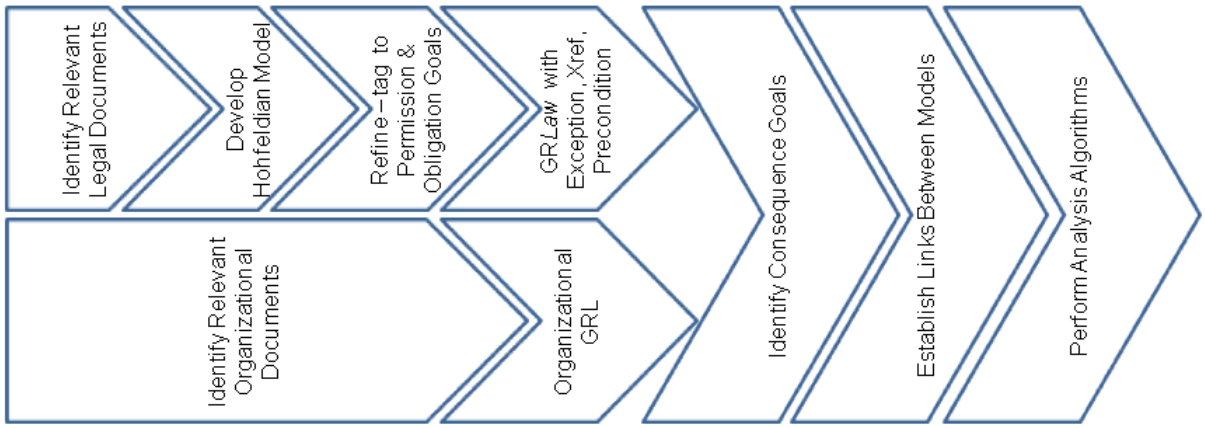

Figure 4.5: Steps Towards Legal and Organizational GRL

4.7 Description of the Layers of the LEGAL-URN Framework - (Steps 1 to 8)

In this part, we explain the steps of the LEGAL-URN framework and define how each layer is built based on those steps.

4.7.1 Step 1 – Identify Relevant Legal and Organizational Documents

The first step includes the process of identifying relevant laws, regulations and standards for the organization as well as related organizational policies and procedural documents.

4.7.2 Steps 2 and 3 – Developing and Refining a Hohfeldian Model of Law

In the next step, which is concerned with the second layer of the framework and only exists only for legal models, we build the Hohfeldian model. For this, we annotate each legal statement in each legal document with one of the Hohfeldian correlative classes of rights. Each statement is therefore assigned one of the following tags: *duty-claim*, *privilege-no-claim*, *power-liability*, or *immunity-disability*.

We use the textual Hohfeldian classification of rights in this layer to analyze legal statements. After a set of refinements, we transform these Hohfeldian classifications into a format that exploits deontic modalities (i.e., Obligation and Permission) at the GRL level. We use a textual format of Hohfeldian classification instead of adopting the *Nòmos* framework for the second layer because the analysis in our framework happens in the third layer, with GRL. *Nòmos* can only be used for transformations from the legal document to Legal GRL model. In our framework, the textual format is used for this transformation and *Nòmos* becomes unnecessary.

To extract Hohfeldian statements from legal documents and build the Hohfeldian model, first, we consider the following rules:

- **Rule 1 -** Each legal statement shall be atomic. This means that each legal statement contains one <actor> (the subject), one <modal verb> (modality), one to many <Clause> (<verb> and <actions>), 0 to many optional <crossreference>, 0 to many optional <precondition> and 0 to many optional <exception>.

- **Rule 2 -** If a legal statement contains more than one modal verb, it needs to be broken down into atomic statements.

- **Rule 3 -** Exceptions are treated as separate statements.

- **Rule 4 -** If there is an internal or external cross-reference in a legal statement, we replace the referencing part of the statement with the referenced statement and break the statement into atomic statements.

Figure 4.6 illustrates the meta-model for the Hohfeldian models. As shown in this meta-model, each Hohfeldian model consists of one to many Hohfeldian statements. Each Hohfeldian statement is an atomic statement and it consist of one subject, one modality, one to many Clauses, 0 to many cross-references, exceptions and preconditions.

Next, we identify Duty-Claim, Privilege-NoClaim, Power-Liability and Immunity-Disability statements based on the potential modalities. Table 4.1 shows a non-exhaustive list of modalities mapped to their respective Hohfeldian classes. The first column represents the classes, the second column represents the modalities for Duty, Privilege, Power and Immunity (one side of the dual relationships) and finally the last column shows the modalities for Claim, No-Claim, Liability and Disability (the other side of the dual relationships).

As shown in Table 4.1, some of the keywords used in defining duty-claim statements include *must, shall, will, have to, is necessary to*, and *can, may, will* for their correlative statements. Those for privilege-noclaim statements include *may, might, should*,

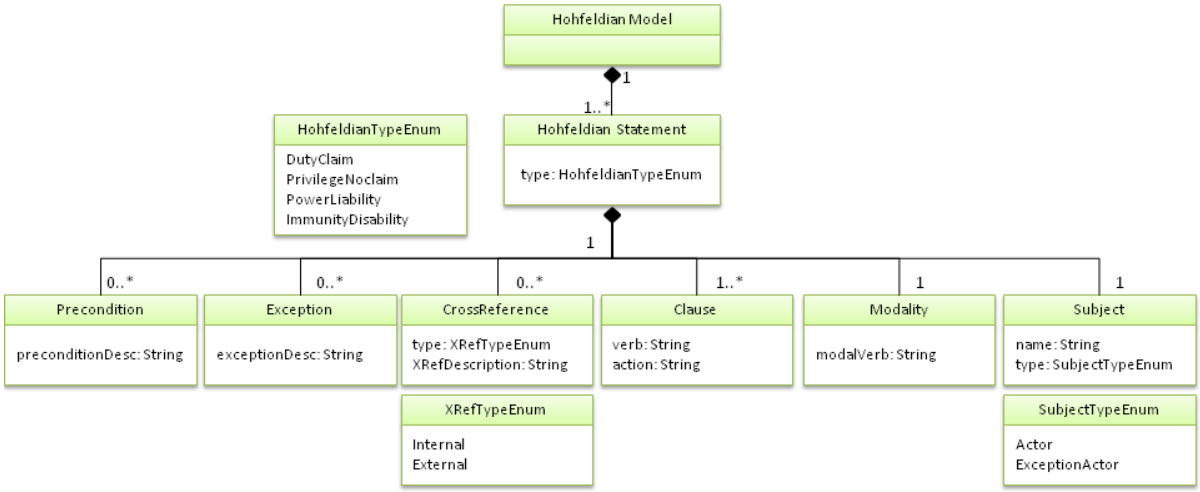

Figure 4.6: Hohfeldian Statement Meta-Model

and *cannot, may not, will not* for their correlative statements. For all classes, other synonyms (including expressions) also exist. As mentioned in Chapter 2, power-liability and immunity-disability are statements that can override the two above statements and they are mainly decomposed into either of the first two types. The power-liability gives a power to the actor to perform an action which was not allowed in a regular situation. This means that the power-liability statements may contain the keywords *must allow actor to, shall authorize an actor to*, etc. Immunity-disability disables an actor from performing an action and prevents him from being penalized. Power-liability and immunity-disability have priority over the duty-claim and privilege-no-claim statements. Note that the lists provided in this table are not exhaustive and there can be many more modalities that can match these classes. Also, these patterns may go beyond the verb-based patterns used here (and could include nouns and expressions). Whether classification can be automated, even partially (e.g., based on natural language processing or predefined patterns or templates) is outside the scope of this thesis.

Table 4.1: Mapping between Hohfeldian Classes and Modalities

Hohfeldian Classes	**Modalities**	**Correlative Modalities**
Duty-Claim	Must Shall Will Have To Is Necessary To Other synonyms	Can May Will Other synonyms
Privilege-Noclaim	May Might Should Is Permitted To Is Allowed To Other synonyms	Cannot May Not Will Not Other synonyms
Power-Liability	Must Allow ... To Shall Allow ... To Shall Permit ... To Shall Authorize ... To Has a Right To Other synonyms	Is Liable to Is Ought to Other synonyms
Immunity-Disability	Must Not Allow ... To Shall Not Allow ... To Shall Not Permit ... To Shall Not Authorize ...To Not Have a Right To Other synonyms	Is Not Able to Other synonyms

Examples of Hohfeldian Models

In order to understand how these models are built, we provide several examples of legal statements transformed to Hohfeldian statements.

Duty - Claim PHIPA article 10(1) states: *"A health information custodian (HIC) that has custody or control of personal health information (PHI)* ***shall*** *have in place information practices that comply with the requirements of this Act and its regulations. 2004, c. 3, Sched. A, s. 10 (1)."*

The different parts of this atomic statement are presented in Table 4.2.

Table 4.2: PHIPA-Article 10

Actor	An HIC
Modal Verb	Shall
Clause (Verb/Action)	Have in place/ information practices that comply with the requirements of this Act and its regulations.
Precondition	Has custody or control of PHI

If the precondition is true, then an HIC *shall* have in place information practices that comply with PHIPA.

Since the modality is *"shall"*, this statement is annotated with a Duty-Claim tag.

Privilege - NoClaim PHIPA article 18(2) states: *"Subject to subsection (3), a consent to the collection, use or disclosure of personal health information about an individual **may** be express or implied. 2004, c. 3, Sched. A, s. 18 (2)."*

This statement provides requirements for consent in the case of collection, use or disclosure. Table 4.3 shows the different parts of the statement based on the meta-model.

Table 4.3: PHIPA-Article 18(2)

Actor	Not defined
Modal Verb	May
Clause (Verb/Action)	Be / express or implied

This statement includes the modal verb, *"may"*, thus, it is annotated with a Privilege-NoClaim tag.

Power - Liability PHIPA Article 52(3) states: *"(3) Despite subsection (1), **if** a record is not a record dedicated primarily to PHI about the individual requesting access, the individual **has a right** of access only to the portion of PHI about the individual in the record that can reasonably be severed from the record for the purpose of providing access. 2004, c. 3, Sched. A, s. 52 (3).*

With this statement, an individual has the *power* to access to a portion of the PHI if it satisfies the precondition. In this case, if the individual asks for accessing his PHI, the HIC has to disclose the PHI to the individual. Therefore, this statement provides power for individual and can override any other relevant statements. The keyword *"has a right"* describes the power-liability Hohfeldian class and it is annotated as a Power-Liability statement.

Table 4.4: PHIPA-Article 52(3)

Precondition	If a record is not a record dedicated primarily to PHI [...]
Actor	Individual
Modal Verb	Has a right
Clause (Verb/Action)	Access only to the portion of PHI [...]

Article 30(2) of "Freedom of Information and Protection of Privacy Act" (FIPPA, 2011) [79] provides another example of a Power-Liability statement: *(2) Where a person requests the opportunity to examine a record or a part thereof and it is reasonably practicable to give the person that opportunity, the head* ***shall allow the person to*** *examine the record or part thereof in accordance with the regulations. R.S.O. 1990, c. F.31, s. 30 (2).*

In this statement, a person has a "power" to examine the record and the head is liable to allow the person to do so. The keyword *shall allow ... to* represents the Power-Liability statement.

Table 4.4 and Table 4.5 show the parts of these two statements based on the meta-model definition.

Immunity - Disability FIPPA Article 12(1) states: *"12. (1) A head* ***shall refuse to*** *disclose a record where the disclosure would reveal the substance of deliberations of the Executive Council or its committees, including,(a) an agenda, minute or other record of the deliberations or decisions of the Executive Council or its committees;(b) a record*

Table 4.5: FIPPA-Article 30(2)

Precondition	Where a person requests the opportunity to examine a record or a part thereof and it is reasonably practicable [...]
Actor	Head
Modal Verb	Shall allow ... to
Clause (Verb/Action)	Examine the record or part thereof in accordance with the regulations

containing policy options or recommendations submitted, or prepared for submission, to the Executive Council or its committees; [...]

This statement has has a keyword *shall refuse to*, which is a synonym of the keyword *shall not allow to*. Because of this keyword, this statement is of type of Immunity-Disability. The head is disabled to disclose a record that can reveal the substance of deliberations [...]. This action provides immunity to the executive council or its committee. Table 4.6 shows the subparts of this statement based on the Hohfeldian meta-model.

Table 4.6: FIPPA-Article 12(1)

Precondition	where the disclosure would reveal the substance of deliberations of the Executive Council or its committees [a..f]
Actor	Head
Modal Verb	Shall refuse to
Clause (Verb/Action)	Disclose a record

4.7.3 Steps 4 and 5 – Developing Legal GRL and Legal UCM Models

In steps 4 and 5, Legal GRL and UCM models are defined. Since most of the analysis of the framework occurs in the GRL layers and not all of the regulations are procedural, we first focus on how to build GRL models of the law from the Hohfeldian models (i.e., Step 4). This GRL model is called *Legal GRL*. For such modeling, we introduce a lightweight

URN profile targeting compliance. This profile will be explained in greater detail in Section 4.8.

Since all four groups of Hohfeldian rights can be transformed in terms of permissions and obligations, we extend the GRL notation to capture two new types of legal goals. To build the Legal GRL model, we create *obligation* and *permission* goals or softgoals as derivatives of the Hohfeldian model in the second layer and then refine these goals until they can be expressed in terms of operationalized tasks.

In addition to these two types of goals and in order to capture preconditions, exception and external cross-references, we introduce three other types of goals: precondition goals/softgoals, exception goals/softgoals and XRef goals/softgoals.

As in conventional GRL models, intentional elements are connected together through *AND-decomposition*, *OR-decomposition*, *XOR-decomposition*, *contribution*, *correlation* or *dependency* links. However, for the Legal GRL model, *Dependency* links and *External URN links* are defined more specifically:

- *Dependency* links are links from a «Precondition» to an intentional element (usually a softgoal or a goal) and are implemented as standard GRL dependency links. *Dependency* links are annotated by a «depends» stereotype.

- *External URN links* (▶) are also used to map an «XRef» goal to an external cross-reference intentional element in another legal model. External *URN* links are annotated by an «external» stereotype.

Note that the links described in this subsection are specific to organizational and Legal GRL models. Source, compliance, responsibility, traceability and consequence links are used to connect different elements of the LEGAL-URN framework together.

Actors in the Legal GRL model can be divided into two types: Actors and Exception-Actors. ExceptionActors need to only be satisfied if the precondition for their exception goals are satisfied. The ExceptionActors have exception goals bound to them.

To build the Legal GRL model, we follow the steps below:

1. Refine Hohfeldian statements into obligation and permission statements.

2. Map obligation and permission statements to obligation/permission goals in the Legal GRL model.

3. Map preconditions, exceptions and external cross-reference statements to precondition, exception and XRef goals in the Legal GRL model.

4. Internal cross-reference statements are modeled as regular obligation/permission goals. There will be a conventional GRL link from the internal cross-reference goal to the main goal to which it is cross-referenced.

5. For an external cross-reference statement, treat the statement as a regular statement, model it in a separate GRL model, and link the high-level XRef goal to the goal that had it cross-referenced.

6. Exception goals must have at least one precondition goal. If the precondition is satisfied, then it triggers the exception goal.

7. Each subject in the Hohfeldian statements is modeled as an actor in the Legal GRL model whereas each exception subject in the Hohfeldian statement is modeled as an exceptionactor in the Legal GRL model.

8. Map actions in the Clause part of an Hohfeldian statement to tasks in the Legal GRL model.

9. Provide links between the goals and tasks in the Legal GRL model as follows:

    - If obligation and permission goals are connected to softgoals, the links are either contribution or decomposition links (i.e., similar to conventional GRL models).
    - If obligation or permission goals are refined into more obligation or permission goals, they are connected through decomposition links.

- Tasks are connected to obligation and permission goals through AND, OR or XOR decomposition links.
- Preconditions are connected to intentional elements through dependency links.
- Exception and XRef goals are treated similarly to obligation and permission goals.

Table 4.7 provides a summary of the mapping between the Hohfeldian model's elements and the Legal GRL model's elements while Figure 4.7 illustrates this mapping.

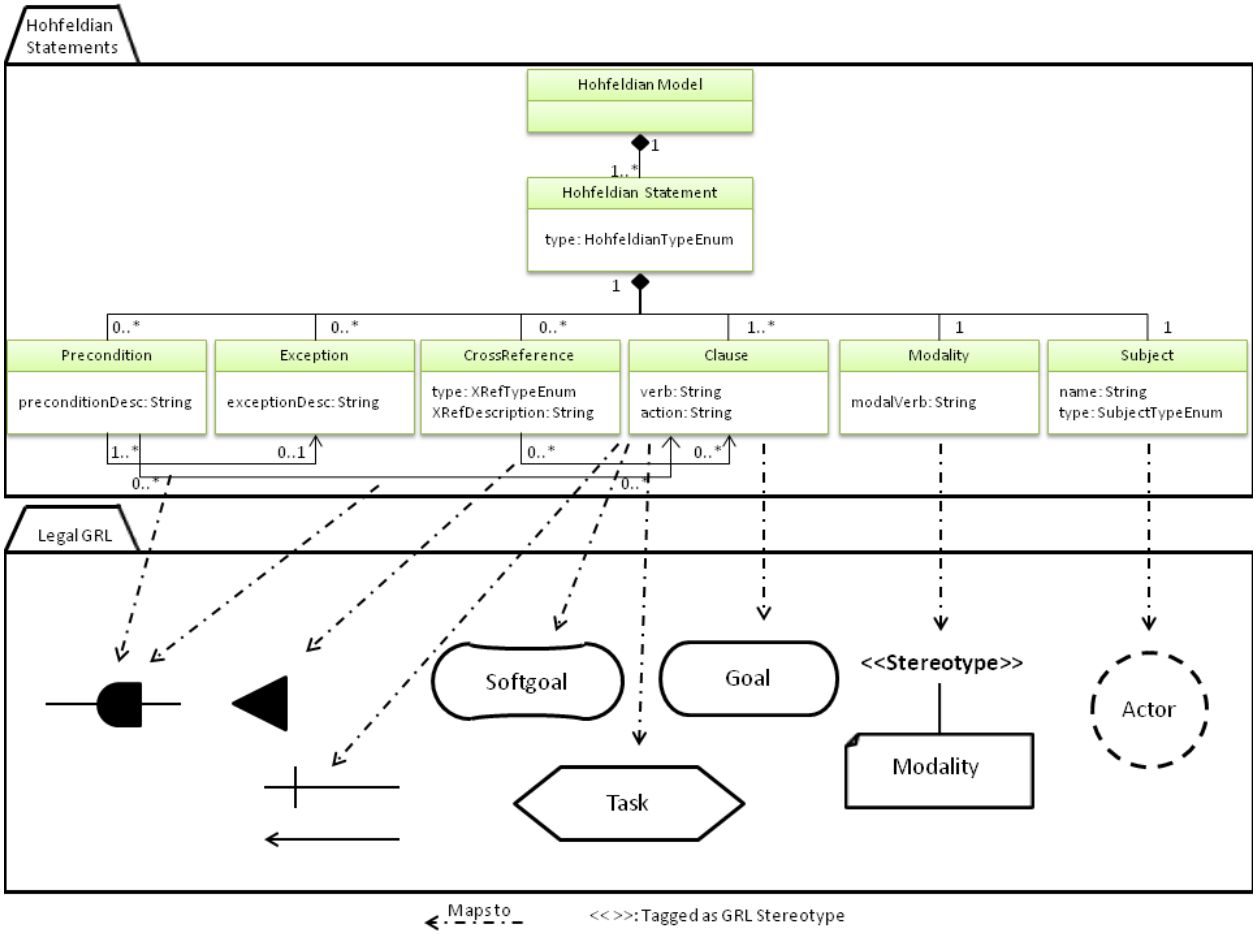

Figure 4.7: Hohfeldian Model and Legal GRL Model Mapping

It is worth mentioning that although other goal modeling notations could be used,

Table 4.7: Summary of Mapping between Hohfeldian Model and Legal GRL

Hohfeldian Model Element	**GRL Element**
Subject	Actor, ExceptionActor (Stereotyped)
Modality	Obligation/Permission Stereotype
Clause	Intentional Elements
Crossreference	XRef Intentional Elements
Precondition	Precondition Intentional Elements
Exception	Exception Intentional Elements

we use GRL in this work since it has the benefit of being linkable to UCM scenarios, and the latter are suitable for representing business and legal processes. In addition, GRL demonstrates good scalability since it is possible to have multiple diagrams and views of a same model with different levels of granularity. Another benefit of GRL is that it captures actors and their goals with the same notation and is able to link these actors with components in UCMs. Furthermore, since actors play an important role in legal statements, GRL can be useful. In GRL, the desired behaviour of actors (the object of legal prescriptions) can be modeled using the same language as the actual behaviour. GRL also benefits from being graphical and therefore provides useful material for analysis and discussion. From an analysis point of view, GRL also supports the definition of strategies as part of the model, which can be exploited by a variety of quantitative and qualitative evaluation algorithms. Finally, GRL is an international standard, yet it includes first-class extension mechanisms that allow it to be tailored to a particular domain, like compliance.

Examples of Legal GRL Model

In this section, we develop the Legal GRL model of Article 12 and Article 36-1C of PHIPA with respect to the steps explained earlier.

Article 12 (1) states that: *An HIC **shall** take steps that are reasonable in the circumstances **to ensure** that PHI in the custodian's custody or control **is protected against***

theft, loss and unauthorized use or disclosure *and* ***to ensure*** *that the records containing the information* ***are protected against unauthorized copying, modification or disposal***.

Based on the rules in Section 4.7.2, this article can be broken into two atomic statements:

- An HIC **shall** ensure that PHI is protected against theft, loss or unauthorized use or disclosure.
- An HIC **shall** ensure that the records are protected against unauthorized copying, modification or disposal.

As mentioned in Section 4.7.2, since these two statements contain the keyword *shall*, they can be classified as *Duty-Claim* statements. Any duty-claim statement is an obligation. Thus, these two statements are mapped to *Obligation* goals, PHI is Protected... and Records are Protected.... Note that the actor in this model is the *HIC*. Figure 4.8 illustrates the Legal GRL model of this article.

Part (2) of Article 12 says: *Subject to subsection (3) and subject to the exceptions and additional requirements, if any, that are prescribed, an HIC that has custody or control of PHI about an individual* ***shall*** *notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.*

This statement contains *shall* keywords. The HIC has to protect the PHI, but if the PHI gets stolen, lost, or accessed by unauthorized persons, then the HIC can avoid further consequences by notifying the individual. Thus, this statement is of kind *duty-claim*. In addition, the statement explains the duty of the HIC. The refinement procedure for this statement is:

Shall notify the individual: Duty-Claim → Obligation Goal (i.e. Notify Individual*)*

The precondition for this obligation goal is: *PHI is stolen, lost or accessed by unauthorized persons.*

This is shown as the precondition goal in Figure 4.8 on the right-hand side (i.e., in

HIC). The precondition is linked to the goal Notify Individual with a dependency link. The reason for using the dependency link is that the goal Notify Individual is dependent on the precondition. If the precondition is not satisfied, the goal does not need to be satisfied.

In the right part of the model (Figure 4.8), there are three contribution links. The goal Notify Individual is connected to PHI is Protected... and to Records are Protected... via *Help* contribution links. This shows that Notify Individual contributes positively to the two softgoals. The last contribution link is from the precondition goal to the softgoal PHI is Protected.... This precondition can *hurt* the softgoal unless the HIC notifies the individual.

The last part of this article, Article 12 (3), indicates that ***If*** *the HIC is a researcher who has received the PHI from another HIC under subsection 44 (1), the researcher* ***shall not*** *notify the individual that the information is stolen, lost or accessed by unauthorized persons* ***unless*** *the HIC under that subsection first obtains the individual's consent to having the researcher contact the individual and informs the researcher that the individual has given the consent.*

This statement needs to be broken into two separate, atomic statements:

- **If** the HIC is a researcher [...], the researcher **shall not** notify the individual that the information is stolen, lost or accessed by unauthorized persons.
- **If** the HIC first obtains the individual's consent to having the researcher contact the individual and informs the researcher that the individual has given the consent, the HIC **may** notify the individual.

The first atomic statement is classified as a *duty-claim* with a precondition while the second statement is of type of *privilege-noclaim*. These two statements are respectively mapped to obligation and permission goals:

Duty-Claim → *Obligation Goal.*

Privilege-NoClaim → *Permission Goal.*

The first statement provides rules for one instance of the HIC, which is the *researcher*. In the Legal GRL model, this actor is an ExceptionActor and the goal Individual Notification by Researcher is the Exception goal. The precondition is still the same as before, which is the PHI is lost or stolen, etc., but limited to PHI used by the researcher. The goal for the first statement is Not Notify Individual whereas for the second statement it is Notify Individual by Researcher. Since only one of these two goals can be achieved, the link between them is an XOR-decomposition.

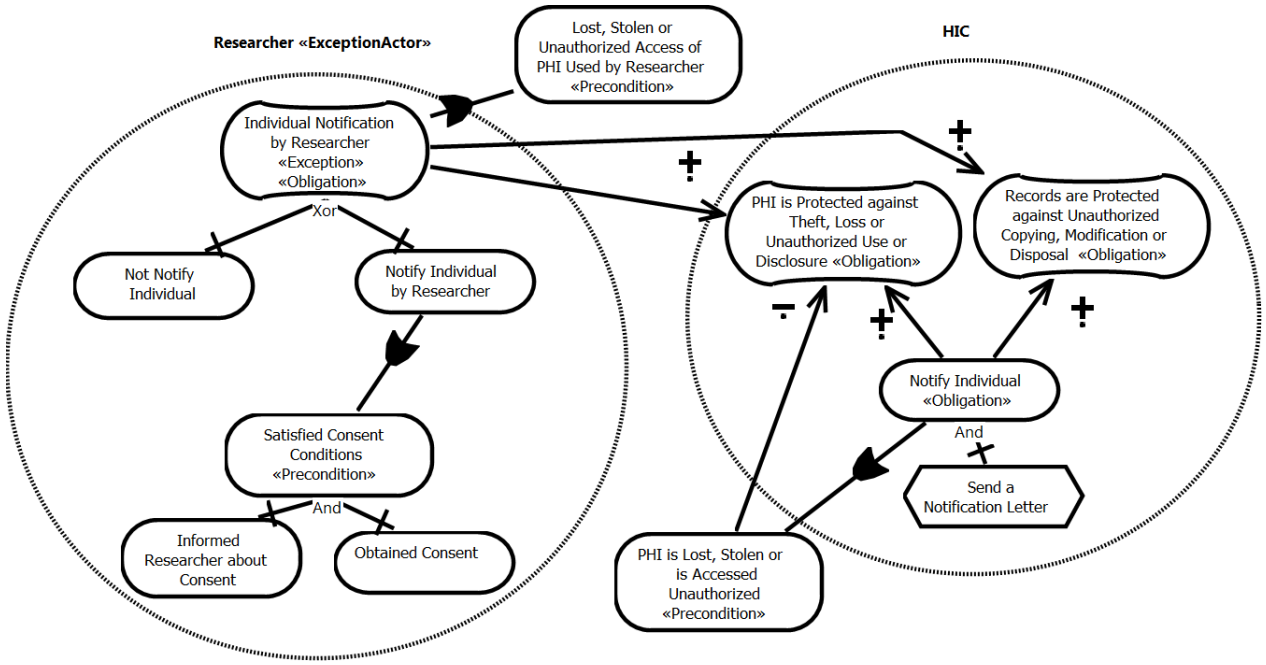

Figure 4.8: Example of Legal GRL Model

To be able to achieve the goal Notify Individual by Researcher, the precondition *HIC (1) obtain individual consent for contacting and (2) inform the researcher* needs to be satisfied. Both parts of the precondition have to be reached at the same time. To show this in the GRL model, we introduce an intermediate precondition goal with an AND-decomposition link from the two sub-goals to this new intermediate goal, and a dependency linking it to the goal Notify Individual by Researcher. The complete model is illustrated in Figure 4.8.

Article 36(1) c states that: *Indirect collection - An HIC may collect PHI about an individual indirectly if, (c) the custodian is an institution within the meaning of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act, or is acting as part of such an institution, and the custodian is collecting the information for a purpose related to, (i) investigating a breach of an agreement or a contravention or an alleged contravention of the laws of Ontario or Canada, (ii) the conduct of a proceeding or a possible proceeding, or (iii) the statutory function of the custodian;*

This article refers to other regulations called FIPPA and MFIPPA [78]. The HIC can collect PHI indirectly if it is defined under these two regulations and also HIC is collecting PHI for the purposes stated in this statement. To be able to show this external cross-reference, we model it as an intentional element HIC is an Institution within Meaning of FIPPA or MFIPPA and annotated it with XRef tag (Figure 4.9).

Then, we identify the cross-referenced article in FIPPA and model it with Legal GRL and provide an External URN link between these two models. In FIPPA, the institution means: *the Assembly, a ministry of the Government of Ontario, a service provider organization, a hospital, and any agency, board, commission, corporation or other body designated as an institution.* Therefore, we model this statement separately and provide an External URN link between them. Figure 4.10 shows this cross-referenced model.

After having built the Legal GRL models, we create the Legal UCM models, if necessary (Step 6). Most legislation is not procedural in nature, but some legislation does describe explicit sequences of activities. In such a case, the legislation specifies procedural constraints. If a constraint contains exceptional situations or actors (which usually represent nested "if" conditions), it cannot be solely shown with GRL, since the latter is only able to depict static representations of goal models. To model these exceptions, we use UCM as this notation is designed to model sequential/causal behaviour such as the one in business processes. The benefit of using UCM over other business processing

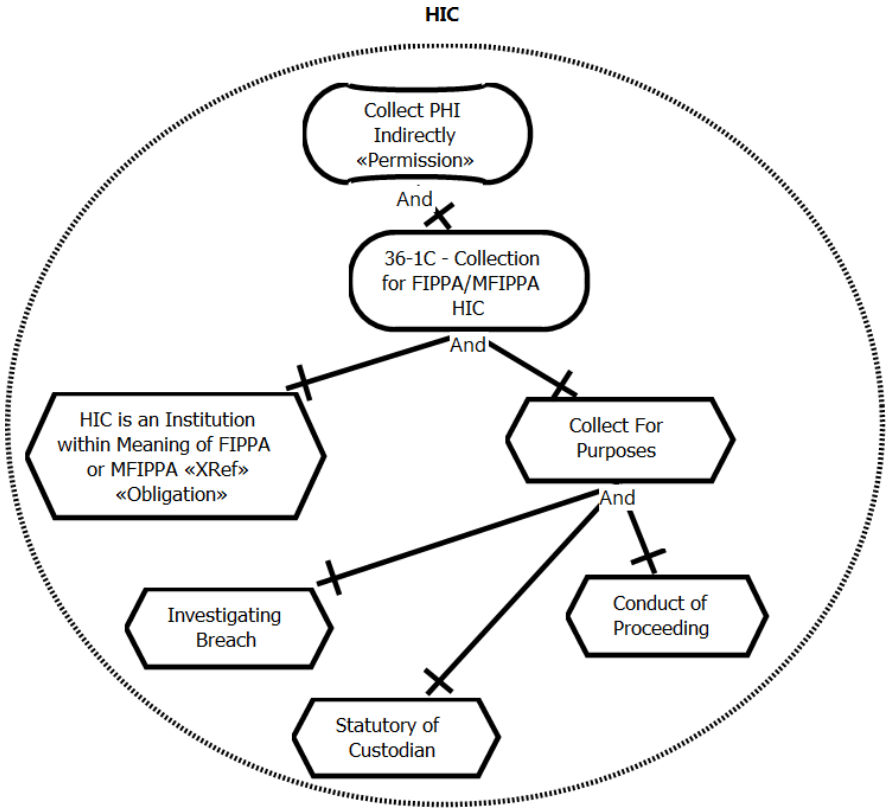

Figure 4.9: Example of External Cross-Reference

modeling notations is that it has the ability to link its elements to GRL elements (as both views are part of URN). In other words, tasks and actors in GRL can be linked to responsibilities and components in UCM maps. Having such business processes for legal clauses helps to capture the sequential aspects of laws and, as a result, this helps to identify violations of the procedural laws.

For example, in PHIPA, article 44 (1)-Disclosure for research indicates that *"An HIC may disclose PHI 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)".* This article mentions that if the HIC permits the access to the PHI after reviewing the documents that the researcher submits, the HIC and the

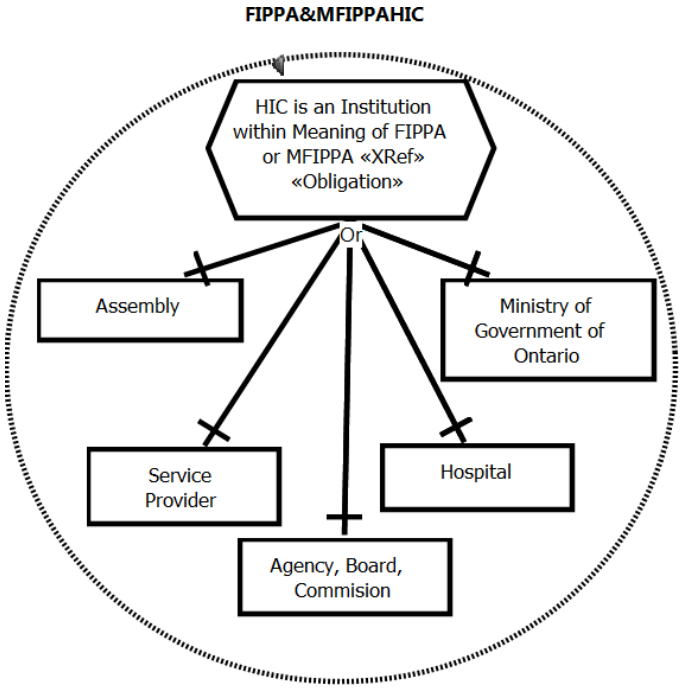

Figure 4.10: Example of External Cross-Reference - FIPPA

researcher need to enter into an agreement. It is evident that this part of the article contains some high-level procedure. Therefore, one of the best ways to show the steps is with a UCM model of the business process. This statement is also modeled in GRL with the URN links (▶) from tasks in GRL to responsibilities in UCM to show the orders of the tasks.

Note that another way of showing the sequences is to add sequence relationship between tasks in goal models [62, 63]. However, we chose to use UCM models to increase the coherence between the organizational and legal model as well as to provide a starting point for organizations to follow while defining their own business processes.

4.7.4 Step 6 – Developing Organizational GRL and UCM Models

In Step 6, we develop organizational GRL and UCM models. In this thesis, we do not cover the process of building organizational GRL models (or strategic goal models) (i.e. Step 6) since this process is covered in much of the existing goal modeling literature from

the last 20 years [15, 66].

As with the organizational GRL model, we do not delve into the details of how to build the organizational UCMs as this process is well documented in the literature [108, 109, 110]. However, it is important to know that *tasks* and other intentional elements in GRL models are mapped to *responsibilities* and *stubs* in UCM models, while *actors* in GRL models are mapped to *components* in the UCMs. The mapping between GRL and UCM models is through URN links (▶)

4.7.5 Step 7 – Defining Consequence Goals and Model

In this step, we define a new type of goal/softgoal named *consequence* goal/softgoal. Consequences aim to capture the potential consequence of non-compliance for organizational goals. Consequences are modeled between the legal and organizational GRL models and they are connected to both legal and organizational intentional elements via *consequence* links. The directions of links are:

- From legal intentional element to consequence intentional element, and
- From consequence intentional element to organizational intentional element.

Figure 4.11 shows an example of a consequence goal linked to organizational and legal intentional elements.

4.7.6 Step 8 – Establishing Framework Links

Table 4.8 presents the summary of the LEGAL-URN framework links which are between the different parts of the framework elements.

In the LEGAL-URN framework, *source* links are used to identify the model elements corresponding to statements of the legal documents.

We also use two different types of *traceability* links: weighted traceability links and simple traceability links.

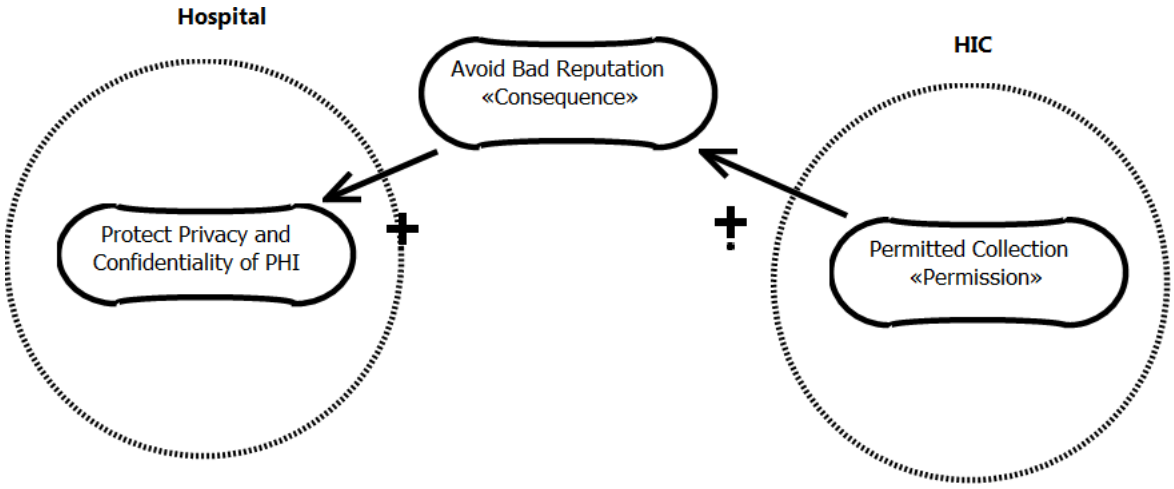

Figure 4.11: Consequence Goal Example

The first type of traceability link (*weighted*) is used to connect the lowest-level intentional elements (mainly tasks) in legal GRL models to the lowest-level intentional elements in organizational GRL models. *Weighted traceability* links are supported by regular contribution links from GRL and hence have both quantitative and qualitative values. *Weighted traceability* links are tagged with the «contributes» stereotype. The quantitative values range from -100 to 100 whereas qualitative values are one of the following: *make*, *help*, *some positive*, *none*, *some negative*, *hurt* and *break*. Through these types of links, the satisfaction values of the lowest-level intentional elements of the organization model (which may be influenced by GRL strategies or by business processes described with UCMs) are propagated to the other intentional elements in the legal model.

The second type of traceability link (*simple*) serves to associate high-level goals in legal GRL models to high-level goals in organizational GRL models. They are used to check if the organization's high-level goals are mapped with the corresponding high-level goals in the legal model. They also allow potential changes in both organization and legal models to be managed. These links are implemented as *URN links* of type «traces». In our models, this type of link is depicted by a dashed arrow to distinguish it from other link types. *Simple traceability* links can also be defined between actors from either type

Table 4.8: Summary of LEGAL-URN Framework Links

Link Name	**Stereotype Name « »**	**Source Element**	**Target Element**
Source	source	Hohfeldian Statements, Legal / Organizational Models	Legal / Organizational Documents
Weighted Traceability	contributes	Organizational GRL / UCM Model	Legal GRL / UCM Model
Simple Traceability	traces	Organizational GRL Model	Legal GRL Model
Compliance	complies	Legal / Organizational GRL Model	Hohfeldian Model
Responsibility	resp	Legal UCM Model, Organizational UCM Model	Legal GRL Model, Organizational GRL Model
Consequence	consequence	Legal GRL Model	Organizational GRL Model

of models. In jUCMNav, the tool used to support our framework, elements with URN links are displayed via a special marker (▶).

Compliance links that are from a Legal GRL model to a Hohfeldian model are used to check if the laws have been modeled correctly and if any statement is missing in the GRL model. *Compliance* links from the organizational GRL model to the Hohfeldian model do not have any weight and are mostly created automatically through traceability links and compliance links. *Compliance* links are described using the «complies» stereotype.

Responsibility links, implemented with URN links, exist between elements of the GRL model and their corresponding elements in the UCM. These links are similar to the links in the URN notation which aim to show the relationship between the intentional elements in GRL and the responsibilities and components in UCM. *Responsibility* links are tagged with the «resp» stereotype.

Consequence links specify the impact of a consequence or penalty arising from cases of non-compliance as defined with respect to the legal model and as it applies to the goals of the organization. These links are of type «consequence» and are implemented as standard GRL contribution links with quantitative and qualitative values.

Simple traceability, *weighted traceability* and *consequence* links are defined between

the two GRL models (organizational and legal). Any other type of link is forbidden between the two GRL models. Such restrictions (acting like an interface) is meant to promote the reusability of the legal model across organizations.

Responsibility links, compliance links, source links and simple traceability links are used to ensure the completeness of the model, to detect missing document's statements in the model, and to manage changes. Weighted traceability links, consequence links, dependency links and URN links are used to analyze the degree of compliance and missing elements in the organizational model. Since it is not possible to insert documents in jUCMNav, both compliance and source links require the use of another traceability tool, such as IBM DOORS (which can handle thousands of linked objects) [23, 25].

4.8 Lightweight URN Profile for Legal Modeling

Since we use goal models for modeling legal documents, GRL plays an essential role in our framework. We discussed in Section 4.7.3 that the legal GRL model contains *permissions*, *obligations*, *consequence precondition*, *exception* and *Xref* goals and softgoals instead of regular softgoals and goals. To be able to include these modalities in the model, we introduce a URN profile for legal models which is called Legal URN profile. In general, the URN standard offers "lightweight" mechanisms (in contrast to more heavyweight mechanisms such as those found in UML) to extend the language. A URN profile takes advantage of three important extensibility concepts:

- **Metadata**, which are name-value pairs used to annotate (e.g., for stereotyping) any model element;
- **URN links**, used to define typed links between any pair of model elements, even across GRL and UCM elements; and
- **Concerns**, used to group any model elements together. Concerns a not really used in our work.

In addition, in a URN profile, well-formedness constraints can be associated with URN elements, including stereotyped and linked ones. These constraints can be formalized in UML's *Object Constraint Language* (OCL) and checked against the model. Analysis and goal evaluation algorithms can also take advantage of profile information [3].

In this section, we describe the lightweight URN profile that we created for implementing the meta-model described in the previous section and hence enable compliance modeling and analysis.

4.8.1 LEGAL-URN Framework Meta-Model Implementation

The meta-model described in Section 4.5 is implemented by URN. Table 4.9 presents the mapping between LEGAL-URN framework meta-model elements and corresponding URN elements.

Table 4.9: Summary of Mapping between Meta-Model and URN

Meta-Model Element	**URN Element**	**Stereotype Value**
Legal Goal Model	GRL Model	«Legal»
Legal Business Process Model	UCM Model	«Legal»
Organizational Goal Model	GRL Model	-
Legal Business Process Model	UCM Model	-

Figure 4.12 shows the implementation of the meta-model with the Legal URN Profile.

4.8.2 Defining Modalities and Consequence Stereotypes – Legal URN Profile

Our profile tailors GRL to capture permissions, obligations, preconditions, exceptions and consequences of non-compliance in legal documents as a generic reference model. To be able to distinguish these special goals from regular goals, we annotate these elements with specific stereotypes. GRL diagrams where legal elements are defined are stereotyped (i.e., tagged with metadata) as «Legal». Any GRL intentional element in a «Legal»

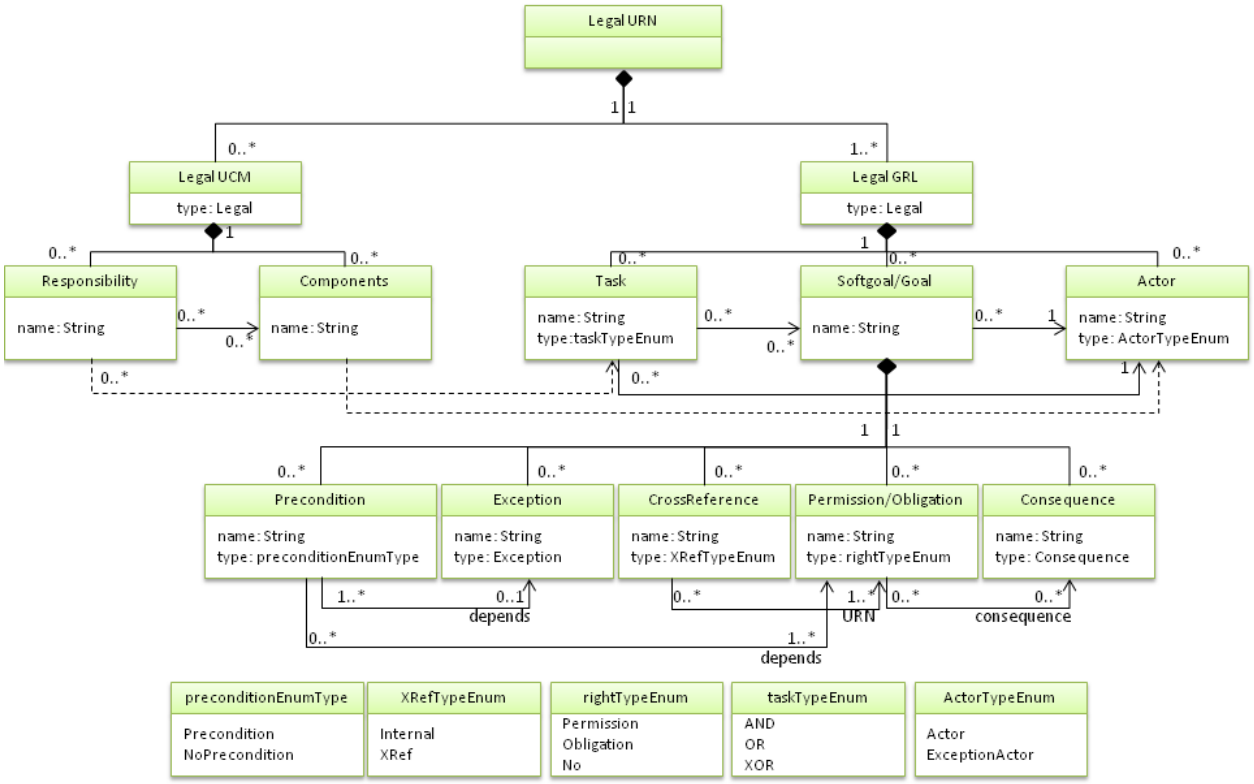

Figure 4.12: Legal URN Profile Meta-Model

diagram, such as goals (⬭), softgoals (☁), and tasks (⬭), that maps to an obligation statement in the legal document will be tagged as an «Obligation» and any goal that maps to a permission statement in the legal document will be tagged as a «Permission».

Furthermore, the profile supports a «Consequence» stereotype used to tag intentional elements in the legal model describing consequences. These special elements have an initial satisfaction value of -100 and cannot be more satisfied than a value of 0, at which time the consequence disappears. GRL contributions from other elements in the legal model to consequences can help avoid them (and hence move up from -100 towards 0).

Another annotation used in the Legal URN profile is the «No» stereotype. The intuition for this stereotype is that not all parts of legal documents are applicable to a single organization. However, since modeling law takes a lot of time, it is easier to

model one legal document once, in a reusable way, and then organizations adapt it as needed. If an organization wants to customize the legal model based on their needs and constraints, it is possible to annotate the irrelevant part of the model with a «No» tag. The elements tagged with «No» are eliminated from the compliance analysis.

The other stereotypes used in the Legal GRL model are «Precondition», «Exception», «XRef», and «NoPreCondition». The «NoPreCondition» is used when the precondition is not applicable during the evaluation and as a result it gets the value of 0.

Permissions and obligations modality tags impose constraints on AND decompositions for the elements that are tagged. In an «Obligation», all the sub-elements of an AND decomposition have to be fully satisfied in order for the tagged element to be satisfied. In a «Permission», though, the sub-elements of an AND decomposition that are irrelevant to the organization (tagged as «No») do not need to be achieved. Furthermore, «Obligation» and «Permission» goals that are not relevant to the organization get «No» tags.

The «Obligation», «Permission», «Precondition», «Exception», and «XRef» tags are part of the model of the law itself (and hence are reusable across organizations as a reference model), whereas the «No» and «NoPreCondition» tags capture, at a given time, which goals or preconditions the organization has not committed to. Hence, elements tagged with «No» and «NoPreCondition» act as if they were not part of the model during evaluations and assessments. Note here that we use quantitative values on a $[-100, 100]$ scale for GRL contribution links. In case of a qualitative analysis, these values are mapped to the corresponding qualitative values as usual.

A summary of the stereotypes, with their values and the URN elements to which they are related, is provided in Table 4.10.

4.8.3 Defining Link Stereotypes – Between Two GRL Models

We explained the various types of links used in the framework in Section 4.7.6. In our URN profile, these links are annotated with relevant tags (metadata) so they can be

Table 4.10: Summary of Legal URN Stereotypes

Stereotype Name	**Stereotype Value**	**URN Element**
ST_Legal	Legal	GRL Model, UCM Model
ST_Legal	Obligation	Softgoal, Goal
ST_Legal	Permission	Softgoal, Goal
ST_Legal	No	Obligation/Permission Softgoal, Goal
ST_Legal	Precondition	Intentional Element
ST_Legal	NoPrecondition	Precondition Intentional Element
ST_Legal	Exception	Softgoal, Goal
ST_Legal	XRef	Softgoal, Goal
ST_Legal	ExceptionActor	Actor, Component

distinguished during modeling and analysis.

The weighted traceability links, which are similar to contribution links, are tagged as «contributes» while the regular contribution links do not have any annotation. The simple traceability links are annotated with «traces» and the consequence links are annotated with «consequences». Compliance links, source links and URN links are tagged with «complies», «source» and «resp», respectively.

4.8.4 Well-formedness Rules

Once a model is built, it can be checked against a set of OCL well-formedness rules. These rules help ensure that the legal models are built correctly and used correctly in conjunction with organization models. The details of this step will be provided in Chapter 5 and Appendix B.1.

4.9 Compliance Analysis Method Overview

After having created all the models and set up the framework, the next step is to determine if the model is compliant with the law. Since most aspects of legal documents are represented in the GRL and UCM legal models, any instance of non-compliance captured

with the two model represents a corresponding violation of the organization to the legal document. Furthermore, the UCM is mainly used to show the procedure, and all of its elements are captured in the GRL model (without the sequence) as well. Therefore, we first focus on the compliance analysis with GRL models. In this section, we provide an overview of the compliance analysis, which will be discussed in detail in the next chapter.

The inputs for our compliance analysis method are:

- legal model(s) described with URN and annotated with the stereotypes described in the previous section («Legal», «Obligation», and «Permission», as well as «Consequences», «Precondition», «Exception», and «XRef»), and
- the organization model, also in URN. Traceability links to the original documents can also be included.

The outputs are:

- a URN model that combines the organization and legal models, together with traceability links, mutual contribution links, dependency links and consequence links and some intentional elements with «No» and «NoPreCondition» tags .
- a sequence of tasks to do in order to become compliant, prioritized according to their complexity and overall impact.

In a nutshell, the steps of the compliance analysis method are the following:

- **Step A.** Tag the goals in the legal model that are not pursued by the organization with the «No» stereotype, with the rationale captured as a belief. In other words, we determine the legal elements that are irrelevant to the organization.
- **Step B.** Specify the links between the two models:
  - Traceability links from the organization model to the legal model(s).
  - Contributions from the organization model to the legal model(s).

  - Consequence impact from the legal model(s) to the organization model.

- **Step C.** Check the well-formedness of the models.

- **Step D.** Add a GRL strategy (possibly with UCM scenarios) describing the as-is situation.

  - Determine the preconditions that are inapplicable to this strategy and tag them with «NoPreCondition» stereotype and capture rationale as a belief.

- **Step E.** Evaluate compliance using a GRL propagation algorithm combined with OCL compliance rules, and diagnose the elements leading to non-compliance (if any).

- **Step F.** Create and evaluate what-if GRL strategies addressing the issues found in the previous step, determine the inapplicable preconditions for each strategy, evaluate and prioritize those that result in full compliance.

- **Step G.** Using the best strategy, prioritize the tasks to be supported.

4.10 Summary

In this chapter, we first discussed the problems that exist in business process compliance and then provided a set of solution criteria. Based on those criteria, we identified the important features of our LEGAL-URN framework and then we presented this framework in detail. Next, we provided a LEGAL-URN framework meta-model for a better understanding of each modeling concept. We also explained each layer of the framework, how to move from textual documents to models, and the links existing between the organization and law models. We also described how URN was tailored for supporting such framework (with a profile) and, finally, we provided a high-level overview of a compliance analysis method to be discussed in the next chapter.

Note that the model construction steps presented here are not necessarily executed by the same person. For example, the creation of the Hohfeldian model and of the Legal URN model for a law can be done by an *expert legal modeler* (e.g., a lawyer with modeling skills) outside the organization, while the organization model can be created by a *business analyst* and the connections between the organization and legal models can be established and exploited for analysis by the organization's *compliance officer*. Having multiple such roles supports separation of concerns and of expertise, and would enable legal models to be created and maintained outside target organizations while being reusable by the latter (i.e., different organizations do not have to re-model laws and regulations when such models already exist). An expert legal modeler could also create and maintain traceability links between multiple regulations. This topic will be revisited later, in Chapter 7.

Chapter 5

A Method for Analyzing the Legal Compliance of Business Processes

In Chapter 4, we explained how to build models for legal compliance in detail. In this chapter, we describe the rules, algorithms and steps necessary for verifying models, analyzing their compliance (quantitatively or qualitatively) and prioritizing instances of non-compliance.

5.1 Compliance Analysis Steps

When the legal model is built, it must be tailored to the context of the organization through tagging and connected to the organization model through typed links (Section 5.2). It is then necessary to verify that the resulting model is well formed, i.e., that it follows a certain structure defined for the framework. This verification is accomplished via a set of well-formedness rules (Section 5.3). If the model satisfies these rules, a strategy describing the as-is situation is defined and the model is evaluated through quantitative or qualitative analysis algorithms (Section 5.4). The non-compliance issues are highlighted by querying the model through a set of compliance rules (Section 5.5). Finally, when the non-compliance instances are identified, a prioritization algorithm helps

to prioritize these non-compliance instances so that the ones with the highest impact are identified (Section 5.6).

Figure 5.1 illustrates the analysis input, output and processes. The input is the output of Chapter 4, where the models of the LEGAL-URN framework are created. The process for producing the output is explained in detail in this chapter, with tool support described in Section 5.7.

To analyze compliance, we adopt GRL analysis algorithms and extend them based on our needs. After identifying the non-compliance instances and prioritizing them, it is also possible to find out which business processes need to be fixed via responsibility links between GRL and UCM models.

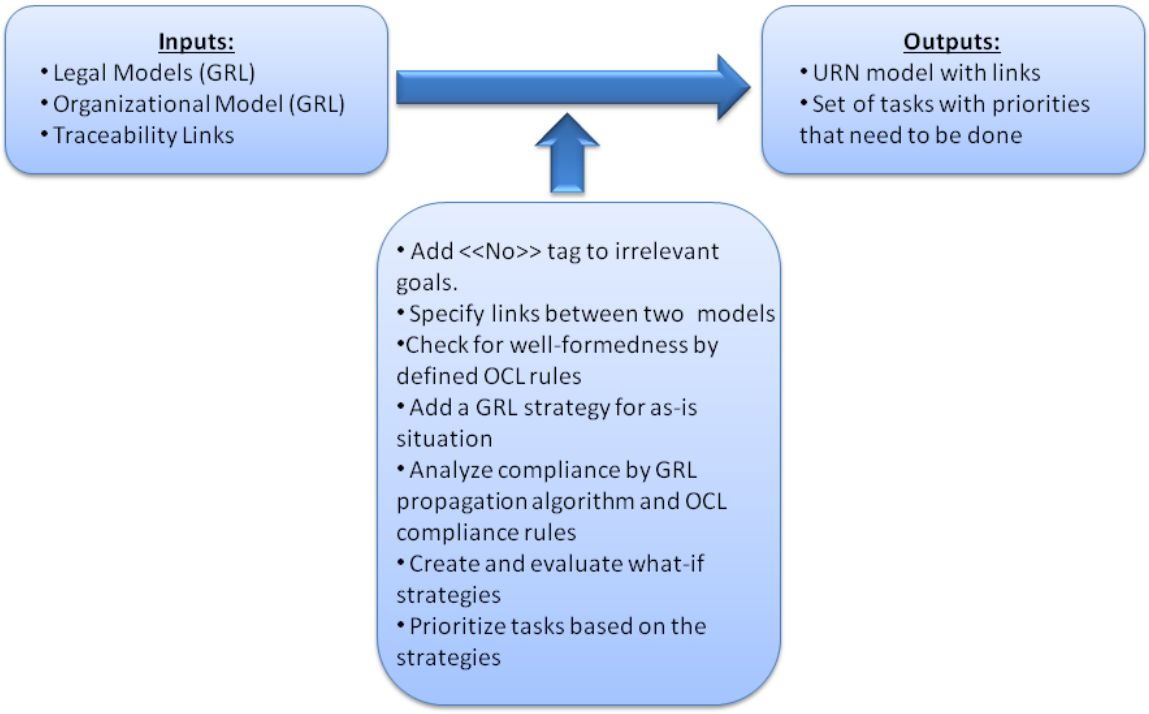

Figure 5.1: Compliance Analysis Steps

5.2 Steps A and B – Annotating Models and Specifying Links

As explained in Section 4.9, in Step A, the legal goals in the legal model that are permitted by law but are not relevant to the organization are tagged with the «No» stereotype and the rationale for the «No» stereotype is captured by a "belief" intentional element in the GRL model.

Then, in Step B, the links between the two GRL models are specified and tagged correctly. These links are of type of *weighted* traceability links (which are similar to contribution links in the regular GRL models), *simple* traceability links and consequence links.

5.3 Step C – Well-Formedness Rules

In Step C, well-formedness rules are used to ensure that the various constraints on the models mentioned so far are formally respected. We define a set of 18 well-formedness rules, written in OCL. These rules are part of the extended URN profile for legal modeling and are supported by jUCMNav.

The rules are as follows:

1. **Rule 1–StereotypeInLegalModelOnly** - If at least one of «Permission», «Obligation», «No», «Consequence», «Precondition», «Exception», «XRef» or «NoPreCondition» stereotypes is used, then it must be referenced in at least one «Legal» diagram. As mentioned earlier, intentional elements in legal GRL diagrams are of type «Permission» or «Obligation», and their violation causes a «Consequence» for the organization.

   Furthermore, an intentional element in a Legal GRL model can be a «Precondition» if it only exists to trigger another intentional element, «Exception» if it only

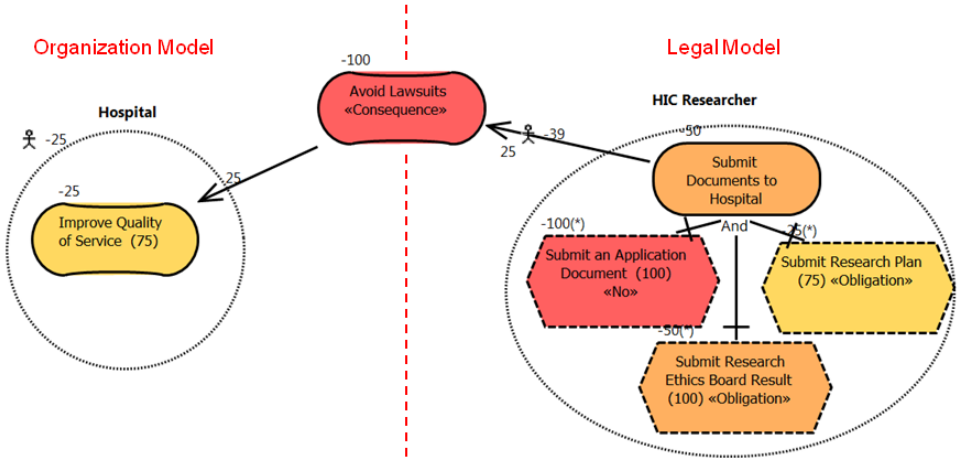

Figure 5.2: Example of Well-formed «Legal» GRL Diagram

occurs under certain conditions, or «XRef» if it refers to a statement from another regulation.

In addition, an intentional element with a «No» or «NoPreCondition» tag only exists for indicating a part of the law that is irrelevant to the organization. These intentional elements differ from the intentional elements that are used in regular GRL diagrams (like those describing the organization). Therefore, in order to have valid models, it is necessary to check that intentional elements with such stereotypes belong to at least one diagram that is stereotyped as «Legal» (i.e., part of the legal model). Refer to Figure 5.2 for an example.

2. **Rule 2–LegalStereo-typesNotForActors** - The «Permission», «Obligation», «Consequence», «Precondition», «Exception», «XRef», «No», and «NoPreCondition» stereotypes are for intentional elements only. Actors and links do not have these types of annotations.

3. **Rule 3–ObligationNotDecomposableByNo** - An «Obligation» intentional element must not be *AND-decomposed* by a «No» element. The reason is that an «Obligation» intentional element means that not performing or satisfying it must result in a violation. As a result, the organization has to make sure that they are

satisfying these types of goals, and their sub-elements when AND-decomposed.

4. **Rule 4–TracesLinksBetweenActors and Rule 5–TracesLinksBetweenIEs** - A «traces» must be between two actors or two intentional elements. These links are "simple traceability" links and they are used to check the compliance of GRL models and manage changes. Therefore, they can only be between two intentional elements, to make sure they are serving the same purpose, or two corresponding actors.

5. **Rule 6–TracesLinksFromOrgToLegalActors and Rule 7–TracesLinksFromOrg ToLegalIEs** - «traces» and «contributes» links must go *from* the organization model *to* the legal model for both actors and intentional elements. In order to find the degree of compliance of an organization to the law, the GRL propagation algorithms are used. Based on the strategies (i.e. GRL analysis algorithms) an organization is taking, the satisfaction values are propagated to other organization model elements and also to the legal GRL model. For this to happen, the links have to be from the organization model to the legal model.

6. **Rule 8–ConsequenceContribFromLegalToOrg** - Only GRL contributions from «Consequence» intentional elements can go *from* the legal model *to* the organization model. Consequences represent the consequence of non-compliance on organizational goals. Therefore, this type of link must be from the legal model to the organizational model (see Figure 5.2).

7. **Rule 9–ConsequenceContribPositive** - GRL contribution links from «Consequence» intentional elements to organization model elements must be positive. Since «Consequence» intentional elements have satisfaction values between -100 to 0 and in order to examine the effect of these negative values on organization goals, contributions links have to be positive. In this case, the value propagated to the organization model will be between -100 and 0, inclusively (see Figure 5.2).

8. **Rule 10–ConsequenceUnused** - «Consequence» intentional elements must have a contribution link to the organization model. Legal consequences cannot be left dangling and must be connected to the organization model.

9. **Rule 11–LegalIEinitialized** - A strategy should not initialize intentional elements from a Legal model. Since the compliance of organization to the legal model is being checked, the strategies are started from organizational intentional elements. **(Rule 11–LegalIEinitialized)**

10. **Rule 12–PreconditionIsDependee** - A «Precondition» must be the target of a dependency link. **(Rule 12–PreconditionIs Dependee)**

11. **Rule 13–PreconditionSatisfactionValue** - A «Precondition» intentional element can only get a value of 0 or 100. A precondition can either be satisfied so that it can trigger the intentional element depended on it or it is not satisfied at all and therefore, the dependent intentional element is not triggered.

12. **Rule 14–XRefHasURNLink** - Every «XRef» intentional element must have at least one «external» URN link to some other element in a different Legal diagram of the model.

The last four well-formedness rules apply to a special diagram part of the legal model that we call *consequence model* (see Figure 5.3). This diagram is required to initialize all the «Consequence» intentional elements of a legal model with a satisfaction value of -100 (DefaultNonComp), and to ensure that their final satisfaction values cannot be above 0 (DefaultMaxEval). This cannot be done through GRL strategies because once initialized by a strategy, the satisfaction value of an intentional element cannot change (and we want it to change for consequences during analysis). The consequence model allows for the constraints on the consequence elements to be respected without changing the GRL propagation algorithms. There is exactly one such diagram per URN model that combines the organization and legal models.

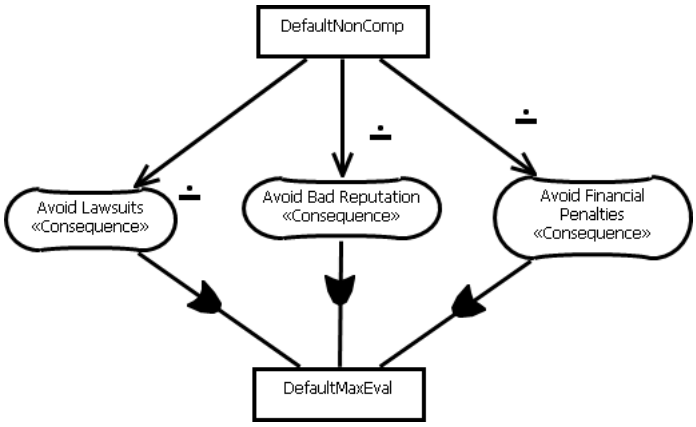

Figure 5.3: Consequence Model

1. **Rule 15–ConsequenceWithMinus100Contrib** - «Consequence» intentional elements must have a −100 contribution from DefaultNonComp.

2. **(Rule 16–ConsequenceDependOnDefaultMaxEval)** - «Consequence» intentional elements must have a dependency to DefaultMaxEval.

3. **Rule 17–DefaultNonCompSetTo100** - DefaultNonComp must be a resource evaluated to 100 in the Legal model.

4. **Rule 18–DefaultMaxEvalSetToZero** - DefaultMaxEval must be a resource evaluated to 0 in the Legal model.

These rules take advantage of an OCL library of over 120 predefined functions used to query and check URN models in jUCMNav [80], hence simplifying the definition of profile rules. These functions allow, among other features, an easy access to element metadata and links. For example, the rule checking that a «traces» URN links from an actor must go to another actor (Rule 4) is defined in OCL as follows:

```
context grl::Actor
inv TracesLinksBetweenActors:
  self.getLinksToForType('traces')
    -> forAll (a | a.oclIsTypeOf(grl::Actor) and a <> self)
```

In turn, this would invoke the library function getLinksToForType():

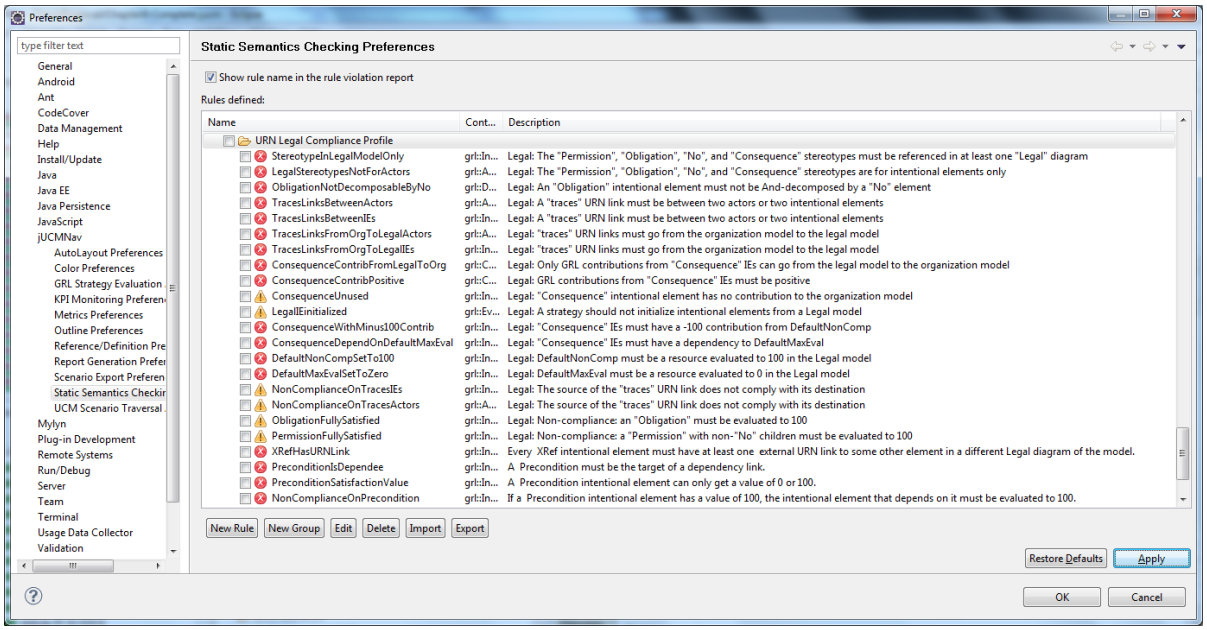

Figure 5.4: jUCMNav Preferences for Selecting OCL Rules to be Checked Against the Model

```
def: getLinksToForType(type:String):Sequence(URNmodelElement) =
-- Returns the URN model elements to which the element
-- links (with the specified type)
  self.fromLinks
    -> select(link:urn::URNlink | link.type = type).toElem
    -> asSequence()
```

The well-formedness rules are all formalized in OCL in Appendix B.1. These rules were added to jUCMNav (some being reported as errors, and the others as warnings). They can be selected through the tool's preferences (see Figure 5.4) and then run at the modeler's convenience.

5.4 Step D – Quantitative and Qualitative Compliance Analysis (Base Strategy)

In the previous section, we defined a set of well-formedness OCL rules to make sure that the URN model comprising the organization and legal models was built correctly. After this step, we need to find the instances of non-compliance, their impact on the organization, and the overall degree of compliance. In order to do this, we start by first giving a base value (quantitative or qualitative) to the lowest level intentional elements in our model and then analyze these elements' degree of compliance (Base Strategy).

After that, to perform the analysis, we use the quantitative and qualitative GRL analysis algorithms that we explained in Chapter 2, and then modify them again to take into consideration the legal aspects (stereotypes) of goal models. One of the main changes in these algorithms is that the intentional elements stereotyped with «No» and «NoPreCondition» are not considered in the analysis. In this section, we explain the quantitative and qualitative GRL analysis algorithms adapted for legal compliance. A qualitative analysis is used when the contribution types and degrees of satisfaction are both qualitative whereas a quantitative analysis is used when they are both quantitative.

As explained in Chapter 2, all three types of GRL analysis algorithms (i.e., quantitative, qualitative, and hybrid) contain the following steps:

1. A GRL strategy initializes quantitative or qualitative satisfaction values of some of the intentional elements (this is done at the lowest level in the GRL model for bottom-up propagation algorithms).

2. These values are propagated to the higher-level intentional elements through decomposition, contribution, and dependency links (in that order),

3. Actor satisfaction values are calculated from the satisfaction and importance of intentional elements embedded in each actor.

Based on the type of algorithm chosen, the result of the analysis can be qualitative (with the qualitative degrees of satisfaction: *denied*, *weakly denied*, *weakly satisfied*, *satisfied*, *conflict*, *unknown*, *none*) or quantitative (with quantitative degrees of satisfaction ranging from -100 to 100).

After analyzing the GRL models quantitatively or qualitatively, these values are propagated to the UCM models through "responsibility" links. As a result, it is possible to identify the non-compliant business processes and modify them.

In our extended GRL analysis algorithm, the GRL strategy initializes the satisfaction values of the lowest-level intentional elements of the GRL model of the organization. Then, these values are propagated to the GRL model of regulations through *weighted traceability* links between the two models. This propagation results in quantitative or qualitative satisfaction values for the intentional elements of the legal GRL model and the overall satisfaction values of the top-level legal goals. Legal consequences and their impact are also computed along the way. Finally, the overall satisfaction values for actors are computed by taking into consideration the importance factors of intentional elements (between 0 and 100 and shown between parentheses).

In order to support steps D to F, we slightly modified these algorithms to take into consideration legal profile stereotypes, in a backward compatible way (i.e., the algorithms behave as before for URN models not based on our legal profile).

One of the modifications pertains to the handling of «No» elements, which are ignored from an evaluation perspective. For example, assume that goal G is AND-decomposed into X, Y, and Z. The normal quantitative algorithm will propagate to G the minimum value among the satisfaction values of X, Y, and Z. However, if G is tagged with «Permission» and Z with «No» then the minimum between X and Y only will be propagated, and Z's value will be ignored. The same approach applies whether we use quantitative or qualitative values. Similarly, for the satisfaction of actors, the elements tagged «No» are simply ignored, whatever their importance levels and satisfaction values.

Figure 5.5 illustrates this modification. In this GRL model, the goal Submit Docu-

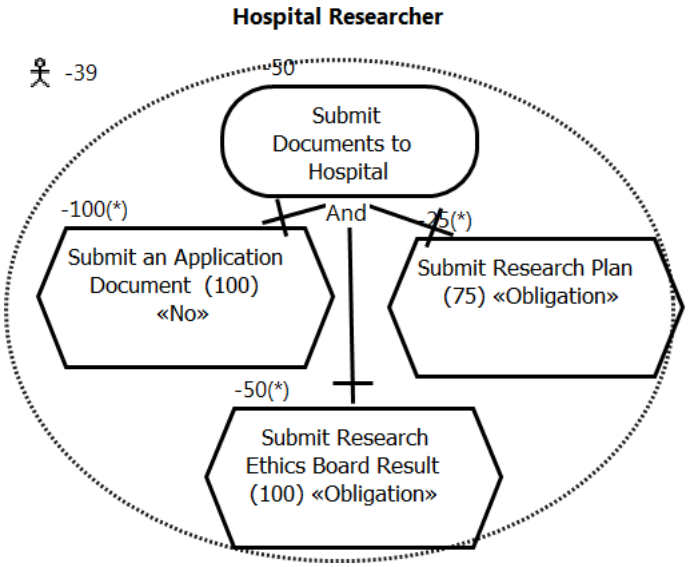

Figure 5.5: Example of Modified GRL Analysis Algorithm

ments to Hospital is AND-decomposed into three tasks. Therefore, the satisfaction value of this goal has to be the lowest value among the tasks linked to it. Among these three tasks, the task Submit an Application Document has the lowest satisfaction value (-100) but it also has a «No» tag. Therefore, its value must be ignored and the satisfaction value of the goal Submit Documents to Hospital becomes the one from the next lowest value, i.e., -50 (from Submit Research Ethics Board Result). Similarly, the satisfaction value of the Hospital Researcher actor is computed from only two of the three tasks with non-null importance levels, i.e., $(75 \times -25 + 100 \times -50)/(75 + 100) = -39$ (instead of -61 without the «No» tag).

The other modification to the algorithm is related to «Precondition» intentional elements handling. As mentioned earlier, if the precondition is not satisfied, the intentional elements connected to it cannot be satisfied and as a result, they have to be removed from the analysis algorithm. To handle the «Precondition» intentional elements, we follow the steps below:

- Define a strategy based on the organization's satisfaction values which propagate to intentional elements of the legal model.

- If the satisfaction value of the «Precondition» intentional element is 0, the intentional element on other end of the dependency link dynamically gets a «NoPreCondition» tag.
- «NoPreCondition» tags are considered as «No» tags in the evaluation algorithm, and hence both are ignored at evaluation time.
- Remove the «NoPreCondition» tags when the strategy is unselected.

5.5 Step E – OCL Compliance Rules

In addition to the 18 well-formed rules, we define 5 new OCL rules to assess compliance and to diagnose non-compliant elements once the GRL model is evaluated by a qualitative or quantitative algorithm. Rules like those that Maxwell et al. suggest [74, 75] can be used to query the model and assess the degree of compliance.

These 5 compliance rules use the satisfaction values of GRL actors and intentional elements evaluated from previous steps and check them against expected values. Model elements violating these rules must be investigated. These rules are as follows:

1. **Rule 19–ObligationFullySatisfied** - An «Obligation» intentional element must be evaluated to 100.
2. **Rule 20–PermissionFullySatisfied** - A «Permission» intentional element with non-«No» children must be evaluated to 100.
3. **Rule 21–NonComplianceOnTracesIEs** - The source intentional element of a «traces» URN link must comply with its destination (i.e., the evaluation value of the link's source must be less than or equal to its destination's).
4. **Rule 22–NonComplianceOnTracesActors** - The source actor of a «traces» URN link must comply with its destination (i.e., the evaluation value pf the link's source must be less than or equal to its destination's).

5. **Rule 23–NonComplianceOnPrecondition** - If a «Precondition» intentional element has a value of 100, the intentional element that depends on it must be evaluated to 100. If that value is less than 100, it is a sign of non-compliance.

These compliance rules are all formalized in OCL in Appendix B.2. These rules were also added to jUCMNav, are selectable through the tool's preferences, and can be verified once the model is evaluated by a GRL propagation algorithm.

5.6 Steps F and G – What-If Strategies and Prioritization Algorithm

In the previous sections, we evaluated the organization model connected to the legal model and provided rules to identify instances of non-compliance. To get closer to being fully compliant, an organization needs to take steps towards removing these instances. However, it may not always be possible, from a practical point of view, to fix these compliance issues all at once. Therefore, it becomes necessary to be able to decide in what order the violations should be resolved. These instances of violations can have different priorities for the organization, and many factors can affect these priorities. For instance, the goals of an organization may not all have the same level of importance. An organization also needs to comply with regulations that affect its capacity to achieve its own goals. Furthermore, not being compliant with the law may lead to negative consequences for organizational goals. However, the degree of impact may again vary from one goal to the next.

In this section, we first identify factors that have an impact on the prioritization of selected goals. We also describe a method to define different strategies for satisfying goals of a legal model and then we propose a formula that evaluates the total priority of any goal in a legal model based on the factors that impact prioritization. Finally, we explain the steps to select the best strategies that address the detected instances of

non-compliance.

5.6.1 Prioritization Factors

There are several factors that can make an activity more important than another one. We identify three such factors:

1. The organization's overall satisfaction level (OrgPr)
2. The legal model's overall satisfaction level (LegalPr)
3. The complexity level of legal clause (task) (ComPr)

It is possible that other relevant factors exist; however, our main goal is to increase the level of compliance of organization to the law while satisfying its own goals in the fastest way possible. Therefore, we only focused on these three factors.

Some goals in an organization are more important than others. For example, in a hospital, improving the quality of care is among the most important goals whereas protecting Personal Health Information may not be as important as the other goal. The goals with the more importance value for organizations get a higher priority than other ones. Achieving these goals will result in a higher satisfaction at the organization level. On the other hand, in case of non-compliance, the organization must deal with a set of negative consequences that hurt the satisfaction value of some organizational goals, resulting in a decreased organization's overall satisfaction level. To mitigate the impact of these negative consequences, organizations must become more compliant with legislation. In GRL, this satisfaction value corresponds to the satisfaction of the target actor and is named OrgPr in our method. Figure 5.6 shows an example of a legal goal "Disclose PHI to Researcher" that contains 3 tasks, a consequence goal, Avoid Lawsuits and two organizational goals, Improve Quality of Service and Protect PHI, whose importance levels are 100 and 90 respectively.

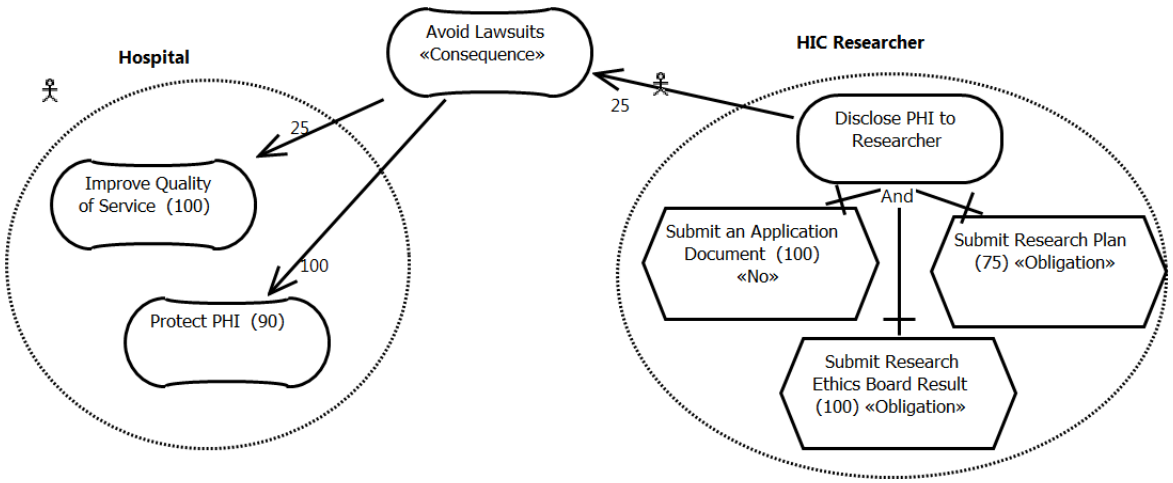

Figure 5.6: GRL Example for Prioritizing Non-Compliance Instances

Furthermore, the degree of satisfaction of the legal model indicates the degree of compliance of the organization with the law. In order for this value to become higher when not fully satisfied, it is necessary to satisfy more legal goals which then indicates that the more tasks related to these legal goals (e.g., through decomposition or contribution links) need to be satisfied. The more required tasks are done, the more likely goals will be achieved and the higher the overall satisfaction value of the legal model which also result on the lower negative consequences on the organizational goals. Determining which set of tasks to perform first will result in different satisfaction values in the legal model. This value is also calculated by the actor's satisfaction level algorithm and is named LegalPr in our method.

In addition, sometimes organizations prefer first to implement tasks that are less complex to get closer to full compliance more quickly and then implement the harder ones. In [72], Massey and Antón defined the level of complexity of a legal statement based on the number of cross-references, the number of exceptions, the number of subsections mapped to, and the number of subsections the statement contains. We reuse this factor in our method and name it ComPr.

5.6.2 Priority Formula

With regards to the selected factors, we define a priority formula. OrgPr and LegalPr can result in quantitative values between -100 and 100 (according to the satisfaction values of their corresponding GRL actor for a given strategy). ComPr however can only get a quantitative value between 0 and 100 (normalized from the value computed by the algorithm in [72]). If a legal statement is very complex, ComPr gets values closer to 0 and if it is less complex then it gets a value closer to 100.

Furthermore, each organization may have different weights (ω_i) for these three types of factors. The weights can be between 0 and 1, and their sum is 1. We only model and analyze quantitative priorities; qualitative values for the actors corresponding to OrgPr and LegalPr are first converted to quantitative values according to a mapping function defined in [2].

The total priority of each statement or element in the model will be calculated as follows:

$Pr = \omega_1 \times OrgPr + \omega_2 \times LegalPr + \omega_3 \times ComPr$; where:

- $0 \leq \omega_1, \omega_2, \omega_3 \leq 1$;
- $\omega_1 + \omega_2 + \omega_3 = 1$;
- $OrgPr$ and $LegalPr$ are in $[-100..100]$; and
- $ComPr$ is in $[0..100]$;

5.6.3 Prioritization Method – What-If Strategies

Based on a given GRL evaluation strategy and the compliance rules, non-compliant «Obligation» and «Permission» goals in a legal model are identified. Then, through the links between these goals and other intentional elements, as well as through the links between the organization and legal models, it is possible to find what is actually missing from the organizational model. For instance, an «Obligation» element that is not satisfied

will likely be so because a sub-element is not satisfied, and eventually such an element will be traced to something not done properly in the organization model, or will not be traced at all, suggesting something is missing from the organization model and its policies or business processes. Figure 5.7 illustrates the base strategy for the example illustrated above (Figure 5.6). As shown in this figure, both tasks Submit Research Plan and Submit Research Ethics Board Result are not performed by the hospital and as a result the legal goal Disclose PHI to Researcher gets the evaluation value 0. The actor HIC Researcher hence gets the value 0, hence LegalPr = 0. Since the legal goal is not satisfied, it has a negative consequence on the organization goals. Both organizational goals are negative, and the actor Hospital gets a negative satisfaction level, and OrgPr = −21.

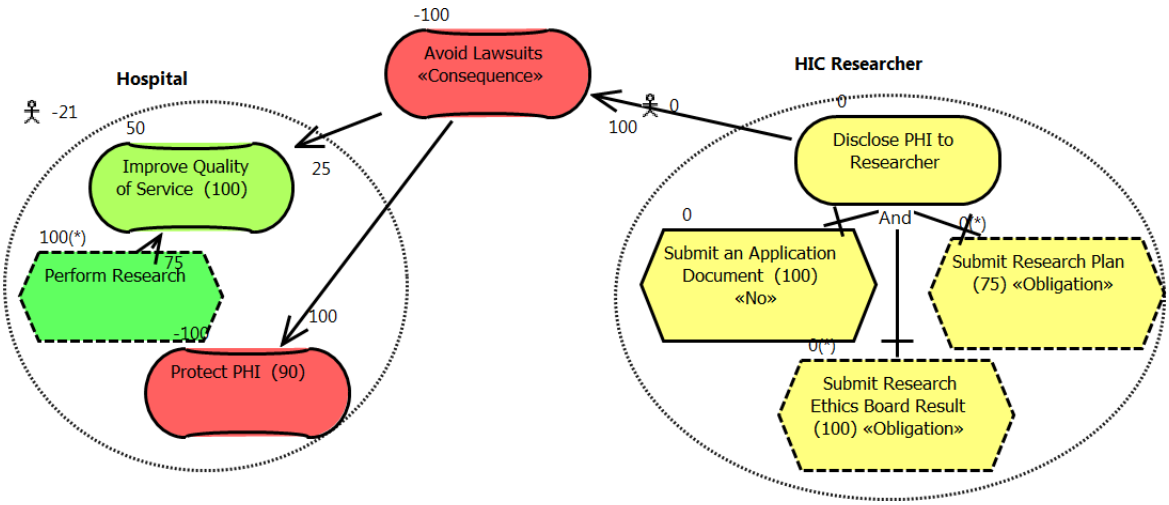

Figure 5.7: Base Strategy

In this step, new GRL strategies are created to determine which subsets of the missing or poorly evaluated tasks are necessary for achieving full compliance. Then, the prioritization method is used to determine the "best" subset as well as the order in which these tasks should be introduced or fixed in the corresponding business processes. This method is as follows: at first, we select one task at a time and find the importance value of legal and organizational actors with respect to their goals and consequences. We repeat this with other strategies where we pick combinations of two tasks at a time, and then three

tasks, and so on until the importance values for all possible combinations are found. This produces OrgPr and LegalPr values for each strategy. In the above example (Figure 5.7) we had two non-compliant tasks. This leads to 3 additional strategies: 2 strategies with one task selected each and one strategy where both tasks are performed. Strategy 1 includes the task Submit Research Ethics Board Result whereas strategy 2 includes the task Submit Research Plan.

Table 5.1: Prioritization Strategies

	Base	Strategy 1	Strategy 2	Strategy 3
OrgPr	-21	-21	-21	39
LegalPr	0	57	42	100
CompPr	100	75	75	50

We then compute and assign a complexity value ComPr to each strategy. The base strategy that includes no new tasks gets the lowest complexity (and the highest ComPr score) whereas the strategy that contains all tasks has the highest complexity (and the lowest ComPr score). In our example, the base strategy with no task gets 100, the two strategies with one task get 75 and the strategy with both tasks get 50. Table 5.1 presents the result of each strategy.

Finally, the weight of each factor is defined by the organization and then the priority value for each strategy (Pr) is calculated. In a strategy composed of more than one task to perform, the priority of each of these tasks will be based on the priority results for the strategy that contains only that task. In our example, we assume $\omega_1 = 0.4$, $\omega_2 = 0.35$, and $\omega_3 = 0.25$.

Pr for each strategy is calculated as:

- Base Strategy: $Pr = (0.4) \times (-21) + (0.35) \times (0) + (0.25) \times (100) = 16.6$;
- Strategy 1: $Pr = (0.4) \times (-21) + (0.35) \times (57) + (0.25) \times (75) = 30.3$;
- Strategy 2: $Pr = (0.4) \times (-21) + (0.35) \times (42) + (0.25) \times (75) = 25.05$;
- Strategy 3: $Pr = (0.4) \times (39) + (0.35) \times (75) + (0.25) \times (50) = 54.3$;

Therefore, in order to satisfy the law, the best strategy is to perform both tasks. However, Strategy 1, which includes task, Submit Research Ethics Board Result, has a higher priority value than strategy 2. Therefore, in the evolution of the business process, it is better to make sure that Submit Research Ethics Board Result is supported first, followed later by task Submit Research Plan.

5.6.4 Discussion on Prioritization Method

The prioritization method introduced here has one limitation: this method is only useful for small organizations or when we have few non-compliance instances, as the number of strategies needed augments exponentially (2^n) with the number of tasks n we can select or not. In this case, the what-if strategies can be very time-consuming, although the rest of the method is done automatically through analysis algorithms and jUCMNav's export mechanism.

To mitigate this problem, it is possible to omit some of the obvious solutions and cluster some of the tasks, leading to a drastic reduction of the number of combinations to check. For example, if two tasks are connected to a higher intentional element through an AND-decomposition, satisfying only one of these task will not change any result in the prioritization and hence such strategy has no added value. Therefore, we do not need to run the strategies for those cases. We can also group several tasks together (e.g., with clusters of 5 tasks each), to reduce the number of strategies, and we can decide to do the most important task of each group and then either re-do the strategies or go to the next ones.

However, such solution can still result in a large number of strategies. Another solution is to avoid using what-if strategies altogether and to adopt and tailor the "GRL Constraint-Oriented Semantic Evaluation Algorithm" discussed in Chapter 2. With this algorithm, we can select a set of high-level Legal goals or high-level Organizational goals, with desired satisfaction values, and the algorithm will identify the Legal tasks needed to be selected to reach those values. However, since this algorithm is in its prototype

phase, we leave the feasibility study of this algorithm as future work.

5.7 Tool Support

We use jUCMNav as our graphical modeling and analysis tool [80, 91]. jUCMNav allows for the definition of metadata/stereotypes, URN links, as well as user-selectable constraints in OCL and multiple evaluation algorithms. jUCMNav hence effectively supports lightweight profiles for URN (and GRL). For our work, we added legal well-formedness and compliance OCL rules to the tool, and we modified the quantitative and qualitative analysis algorithms of jUCMNav to support our new legal stereotypes.

We used this legal profile-aware tool for our case studies explained in Chapter 6 and Chapter 8.

5.8 Summary

In this chapter, we discussed the steps towards achieving legal compliance. First, we provided 18 formal well-formed rules that help ensure the models are built correctly. In the next step, we explained the modified quantitative and qualitative analysis algorithms used to calculate the degree of compliance with the law. To identify instances of non-compliance, we provided another set of 5 OCL rules for compliance assessment. Finally, we introduced an algorithm to prioritize the non-compliant instances. We also briefly discussed our tool support for this compliance methodology.

The next chapter introduces a first case study from the healthcare sector focusing on one organization and one law. It will help illustrate and validate the modeling and analysis techniques presented so far.

Chapter 6

Case Study 1: PHIPA and The Ontario Hospital

In this chapter, we explain the first case study we undertook to validate our proposed model-based compliance framework. This case study was developed incrementally and it illustrates how our models work and demonstrates the steps necessary to manage business process compliance. We first give an overview of the case study (based for the most part on a real hospital, but anonymized here), and then discuss how to model both the law and the organization. Then, we show how to follow our method step by step for achieving legal compliance, including analysis of business processes and prioritization of compliance steps.

6.1 Case Study Overview

In this case study, a research hospital in Ontario, Canada, is dealing with Personal Health Information (PHI) to achieve its high-level goals. The hospital's high-level goals are to provide better healthcare, increase understanding of public health, minimize cost, improve quality of services, and protect privacy and confidentiality of PHI.

To achieve these high-level goals, the hospital collaborates with internal healthcare

researchers as well as external researchers to provide better healthcare, to improve the quality of its services and minimize their cost. In addition, the hospital is involved in activities such as investigating a breach, obtaining payment, or processing, monitoring, verifying or reimbursing claims. However, the hospital is not involved in fundraising, marketing activities or any other programs as such.

For all of these activities, the hospital needs to collect, use or disclose PHI. However, since such PHI is sensitive, the hospital has to ensure the accuracy, privacy and security of the data while ensuring that consent is obtained from patients (implicitly or explicitly). Therefore, in order to collect, use or disclose PHI for any of the above purposes, the hospital needs to comply with the corresponding parts of the relevant regulations. Being compliant and effective in sharing information at the same time is quite challenging and requires a review of (and modifications to) current processes. If the hospital fails to be compliant, they have to deal with some negative consequences, some of which are financial penalties, loss of reputation, and involvement in lawsuits.

To ensure that the hospital is compliant with the relevant regulations while being able to achieve its own mission and business objectives, we model the situation with our Legal-URN framework (Chapter 4). First, we identify the relevant regulations and their relevant parts. Then, we classify the legal statements based on the Hohfeldian classes of rights and identify obligation and permission goals. Next, we build the Legal GRL and Legal UCM models as well as organizational GRL and UCM models. We, then, establish links between these models. Finally, we analyze the compliance and prioritize non-compliant instances based on the methodology explained in Chapter 5.

6.2 Step 1 – Identify Relevant Legal and Organizational Documents

As specified in Section 6.1, our case study is related to the collection, use and disclosure of PHI by hospitals, healthcare organizations and researchers in the province of Ontario,

Canada. The regulation that applies to this case study is the *Personal Health Information Protection Act* (PHIPA), 2004 [40]. PHIPA is the regulation related to healthcare privacy in Ontario. It substitutes the Government of Canada's *Personal Information Protection and Electronic Documents Act in healthcare (PIPEDA)* [37].

PHIPA is based on 10 principles from the *Canadian Standards Association Model Code for the Protection of Personal Information* [18]. These principles are: Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure and Retention, Accuracy, Safeguards, Openness, Access, and Challenging Compliance. PHIPA includes seven main parts and two additional parts (i.e., "Complementary Amendments", and "Commencement and Short Title") as well as 75 articles [77]. The first six articles are related to "Purposes, Definitions and Interpretations" and the next three articles are concerned with the "Application of Act".

PHIPA applies to *Health Information Custodians* (HIC)s who collect, use and disclose PHI, and to any non-HIC who receives PHI from an HIC. PHIPA overrides any other act in the case of conflict unless it is stated otherwise [77].

The hospital also has documents for policies and procedures, which define its objectives, goals and business processes. We use these documents to create organizational GRL and UCM models.

Note that in this chapter, we only work with one regulation. Dealing with multiple laws is covered in Chapters 7 and 8.

6.3 Steps 2 and 3 – Developing and Refining a Hohfeldian Model of Law

With respect to the hospital duties explained above, we examine 18 articles of PHIPA which are related to these duties (e.g., collecting and disclosing PHI to healthcare providers and researchers, investigating breaches, payments, etc.) and identify the type of *right* of each statement based on the Hohfeldian taxonomy discussed in Section 2.2.2.

In Section 4.6, step 2 classifies each statement of the legal document based on Hohfeldian classes of rights, namely Duty-Claim, Privilege-NoClaim, Power-Liability and Immunity-Disability. Each article in PHIPA includes several statements and sub-statements that fall into one of these four categories. Step 3 refines the Power-Liability and Immunity-Disability statements into multiple Duty-Claim or Privilege-NoClaim statements and builds the Hohfeldian model. Note that the number of Power-Liability and Immunity-Disability statements is very small in PHIPA in general, and none were present among the selected articles.

In total, we had 28 Duty-Claim statements mapped to «Obligation» goals and 30 Privilege-NoClaim statements mapped to «Permission» goals.

In this case study, the hospital was dealing with the collection, use and disclosure of PHI. Articles 29 and 31 provide general rules for the collection, use and disclosure of PHI, and for consent:

Requirement for consent - 29. An HIC ***shall not*** *collect, use or disclose PHI about an individual* ***unless****, (a) it has* ***the individual's consent*** *and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge,* ***is necessary*** *for a lawful purpose; or (b) the collection, use or disclosure, as the case may be,* ***is permitted or required*** *by this Act.*

Use and disclosure of personal health information - 31. An HIC that collects PHI in contravention of this Act ***shall not*** *use it or disclose it* ***unless*** *required by law to do so.*

In Article 29, the HIC *shall not* collect, use or disclose PHI but *if* one of the statements below is satisfied, then the HIC *may* collect, use or disclose the PHI (exception):

Precondition a: It has consent, and it is necessary or

Precondition b: It is permitted or required.

Therefore, the statement is of type Duty-Claim however, the exception part of it provides privilege to the HIC and has Privilege-NoClaim in its nature. Table 6.1 shows how this statement was decomposed according to our meta-model.

Article 31 is also of type Duty-Claim with one exception under which the article

Table 6.1: PHIPA-Article 29

Actor	An HIC
Modal Verb	Shall
Clause	Not collect, use or disclose PHI about an individual
Exception	Unless = May collect, [...]
Precondition 1	It has the individual's consent, and the collection, use or disclosure [...] is necessary
Precondition 2	The collection, use or disclosure is [...] permitted

becomes of type Privilege-NoClaim. Table 6.2 summarizes this statement along the structure imposed by our meta-model.

Table 6.2: PHIPA-Article 31

Actor	An HIC
Precondition	that collects PHI in contravention of this Act
Modal Verb	Shall
Clause	Not use it or disclose it
Exception	Unless = May use it or disclose it
Precondition	Required by law to do so

Furthermore, Article 29 requires the HIC to have consent. In PHIPA, Article 18 contains the general rules for consent concerning the PHI. Therefore, Article 29 is internally cross-referencing Article 18. Hence, the hospital must comply with requirements of Article 18 at the same time as Article 29. Article 18 is described in Appendix C, Section C.4.

PHIPA has some other articles for collection, use or disclosure of PHI. However, in our case study, as we mentioned earlier, the hospital *may collect, use or disclose* PHI for only certain purposes and to only some groups, each of which requiring hospital compliance with a corresponding part of PHIPA as follows:

- Falls into indirect/direct collection purposes ⇒ "Collection - Indirect collection or Direct collection without consent" (Article 36, see Appendix C.5).
- Falls into permitted use ⇒ "Permitted use" (Article 37, see Appendix C.6).

- To healthcare providers ⇒ "Disclosures related to providing healthcare" (Article 38, see Appendix C.7).
- To researchers ⇒ "Disclosure for research" (Article 44, see Appendix C.8).

Beside the articles above, the hospital must also comply with the general rules to protect PHI as stated in Articles 10, 11 and 12 of PHIPA (see Appendices C.1, C.2 and C.3).

On the other hand, in our case study we decided that our hospital does not collect use or disclose the PHI for fundraising (Article 32), for marketing (Article 33), for health or other programs (Article 39), for risk, proceeding, successor (Articles 40-42), for planning and management of the health system, monitoring healthcare payments, for analysis of health systems (Articles 45-47) or any other purpose.

By eliminating these articles, we ended up with 30 statements including 17 Duty-Claim and 13 Privilege-NoClaim statements. These articles are discussed in detail in Appendix C.

6.4 Steps 4 and 5 – Developing Legal GRL and Legal UCM

After identifying the relevant articles and the Hohfeldian classes of rights, we build the Legal GRL and Legal UCM models for those articles. To obtain the Legal GRL models, we follow the steps explained in Section 4.7.3. In the first step, each Duty-Claim statement identified in the Hohfeldian model is transformed to an «Obligation» goal while each Privilege-NoClaim statement is transformed to a «Permission» goal.

As mentioned in Section 6.3, the hospital needs to comply with Article 29. In addition to this article, the hospital is required to comply with relevant parts of Articles 10, 11, 12, 18, 36, 37, 38 and 44.

In this section, we first model Article 29, and then identify its relationships to the other articles.

Article 29, as shown before, is of type Privilege-NoClaim. In the Legal GRL model, this statement is mapped to the «Permission» softgoal Collect, Use or Disclosure PHI with two alternative conditions. Figure 6.1 represents this statement.

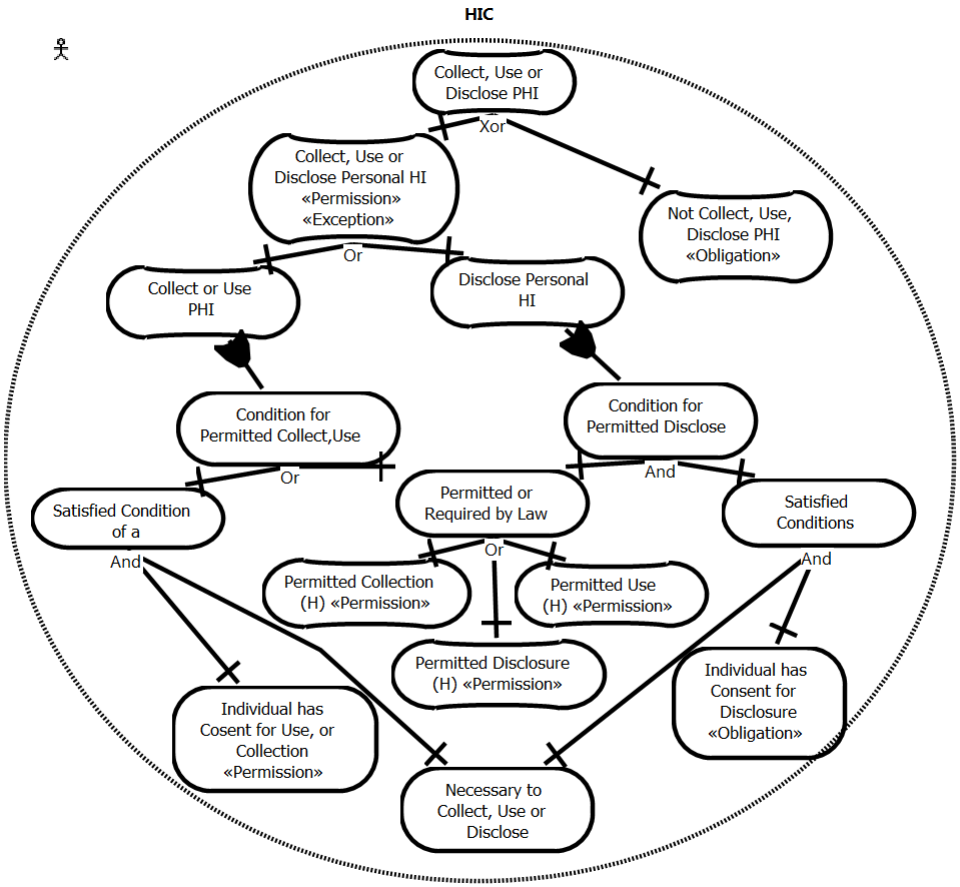

Figure 6.1: GRL Model of Article 29-PHIPA

Article 29 is also related to Article 18 (Figure C.4) since Article 18 discusses the requirements for implied or explicit consent. However, the requirements for consent in the case of collect or use can be different from the requirements for disclosure. To be able to correctly cross-reference these two articles to each other, we decomposed the «Permission» softgoal Collect, Use or Disclose PHI into two softgoals, Collect or Use PHI and Disclose Personal HI. In the Legal GRL model of Article 29, the goals/softgoals for

consent have the same names as the goals/softgoals for consent in Article 18 (these are actually different references to the same GRL element definitions). In this way, until at least one of these two softgoals of Article 18 is satisfied, high-level goals of Article 29 cannot be satisfied. These two softgoals together with the goal Necessary to Collect, Use or Disclose make the first condition (a).

Condition (b) is divided into three softgoals: Permitted Collection refers to Article 36, Permitted Use refers to Article 37, and Permitted Disclosure refers to Articles 38-50. In our case study, for permitted disclosure, we only deal with Articles 38 and 44. Therefore, the other articles related to Permitted Disclosure count as irrelevant. In the Legal GRL models, these softgoals are annotated with «No».

Figure 6.2 illustrates the high-level GRL model for disclosure in general. The high-level softgoal of Permitted Disclosure is annotated with «Permission». This means that disclosure of PHI for each of the softgoals related to it is permitted (i.e., it is permitted by PHIPA that the HIC discloses PHI to the healthcare provider, fundraising agencies, researchers, etc.). When the hospital discloses PHI to researchers, or healthcare providers, it is obliged to follow a set of rules under those statements.

Appendix C describes Legal GRL models of Articles 10, 11, 12, 18, 36, 37 and 38. In this section, we provide details about Article 44, which is the main focus of our case study.

Article 44 - Disclosure for research mentions that *(1) An HIC **may disclose** PHI 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 (REB) that approves the research plan; and (b) enters into the agreement required by subsection (5).*

Statement 44(1) gives permission to the HIC to disclose PHI to the researcher if the researcher performs a set of actions. Therefore, according to the legal ontology in Section 2.2.2, this statement is of type of Privilege-NoClaim and is refined as a «Permission» goal for HIC.

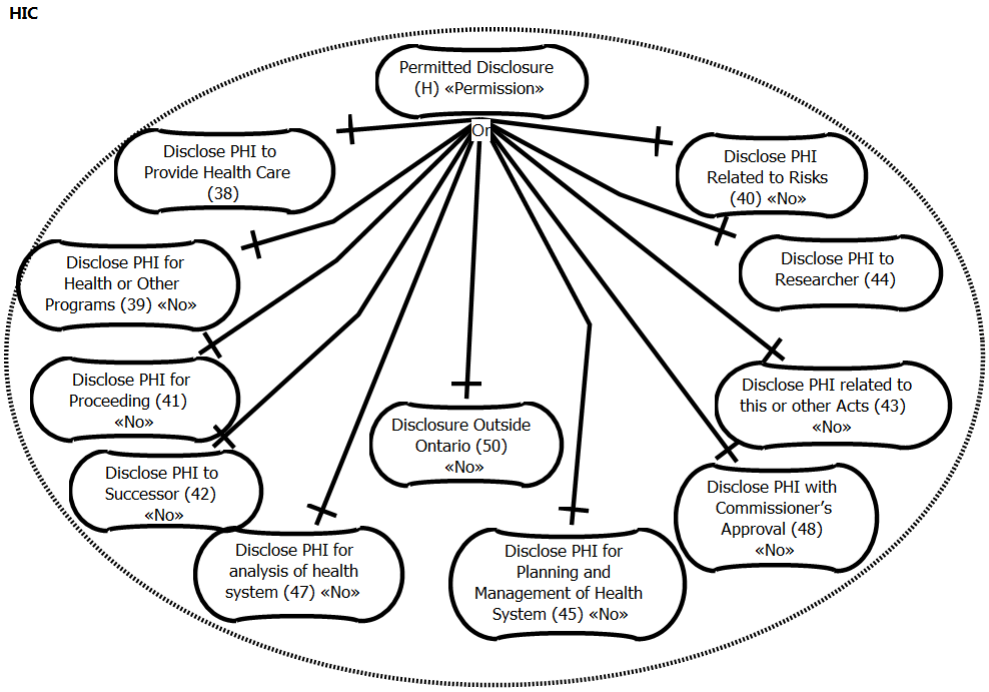

Figure 6.2: Permitted Disclosure - Articles 38-50

Three actors are mentioned in this article: HIC, researcher and REB. Thus, we modeled them in the Legal GRL model for Article 44(1). However, some of the requirements and actions for researchers and the REB have been stated in the other statements of Article 44. Figure 6.3 shows the Legal GRL model for Article 44(1).

As seen in Figure 6.3, the researcher needs to submit a research plan, which is shown as an «Obligation». Statement 44(2) identifies the requirements for the research plan in the form of a Duty-Claim statement (Figure 6.4):

Article 44(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.*

Furthermore, the researcher needs to submit the approval decision from the REB. The considerations for the approval and the decision process for REB are mentioned in Articles 44(3) and (4) below:

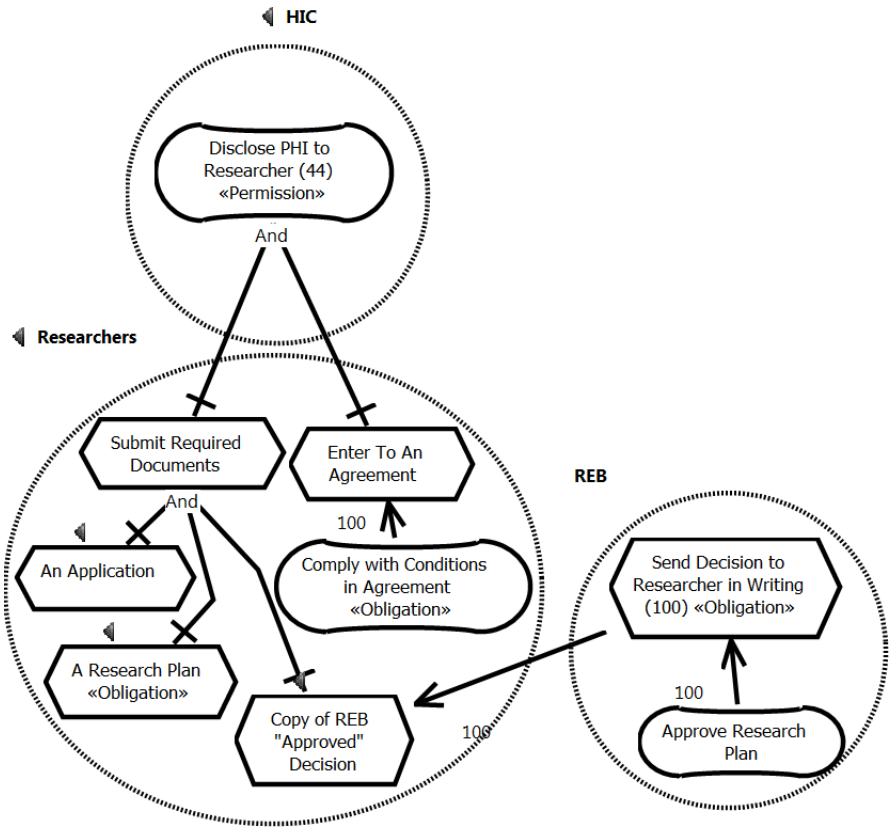

Figure 6.3: Article 44(1) - Disclosure to Researcher

Article 44(3) - **Consideration by board** - *When deciding whether to approve a research plan that a researcher has submitted to it, an REB* ***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.*

Article 44(4) - **Decision of board** - *After reviewing a research plan that a researcher has submitted to it, the REB* ***shall*** *provide to the researcher a decision in writing, with*

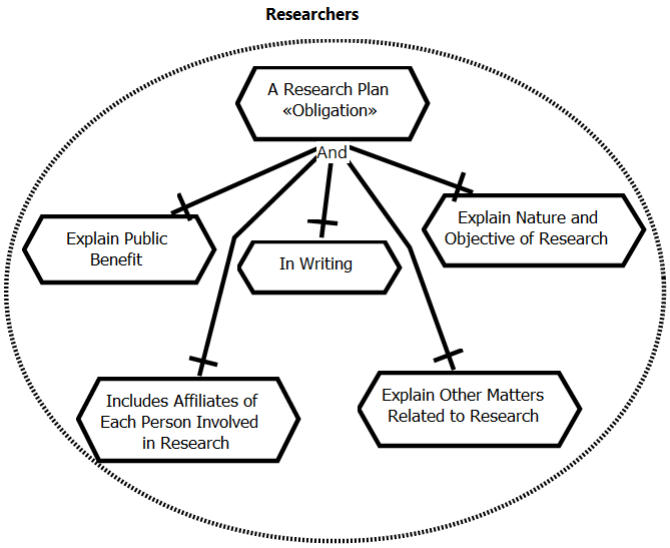

Figure 6.4: Article 44(2) - Research Plan

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.

These two statements are defining the duties of the REB and are Duty-Claim statements. Figure 6.5 shows the Legal GRL model of statements 44(3) and 44(4).

Also, Articles 44(1) and 44(5), state that the researcher needs to enter into an agreement. Article 44(5) refers to a set of conditions that the researcher must comply with. These conditions are defined in statement 44(6).

Article 44(5) - **Agreement respecting disclosure** - *Before an HIC discloses PHI 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.*

Article 44(6) - **Compliance by researcher** - *A researcher who receives PHI about an individual from an HIC* ***under subsection (1) shall****: (a) comply with the conditions, if any, specified by the REB in respect of the research plan; (b) use the information only for the purposes set out in the research plan as approved by the REB; (c) not publish the information in a form that could reasonably enable a person to ascertain the identity*

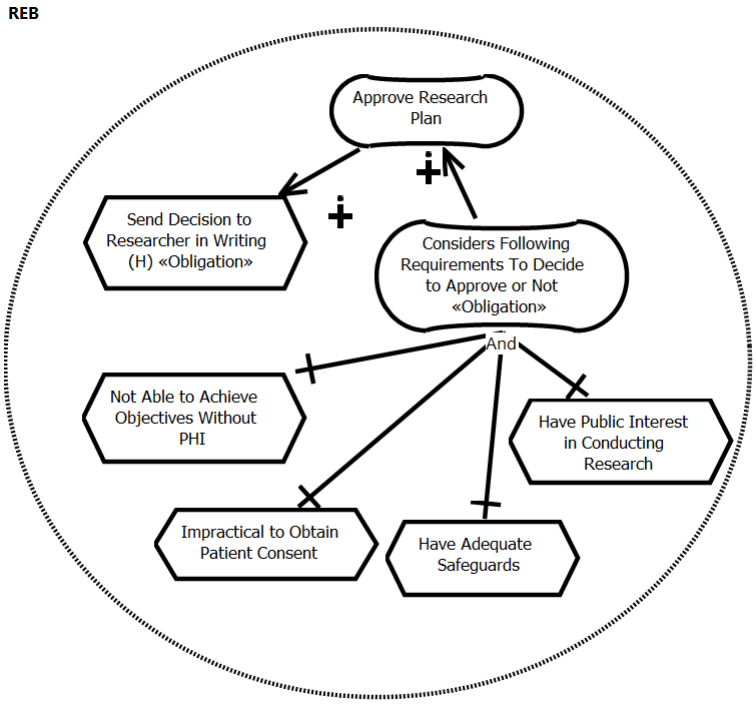

Figure 6.5: Article 44(3,4) - REB Considerations and Decision

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).

Both statements 44(5) and 44(6) are Duty-Claim statements, which are modeled as «Obligation»s in the Legal GRL model (see Figure 6.6).

In addition to the Legal GRL model, Article 44 provides a procedure for disclosure to the researcher. This article states that the researcher has to submit a set of documents to HIC, the HIC has to review them and if they are accepted, the researcher and the HIC have to get into an agreement. The model of this process was built with the UCM notation. Components of the Legal UCM model were linked to actors of the Legal GRL

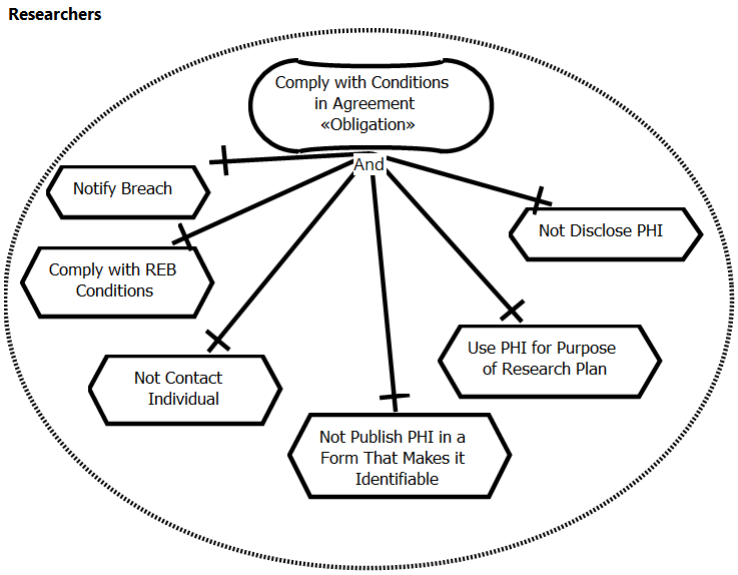

Figure 6.6: Article 44(5,6) - Agreements Compliance

model while responsibilities and stubs in the Legal UCM model were linked to tasks of the Legal GRL model via *URN* links (whose presence is indicated by dark triangle symbols). Figures 6.7 and 6.8 illustrate this process. The rest of the models and the relevant articles are shown in Appendix C.

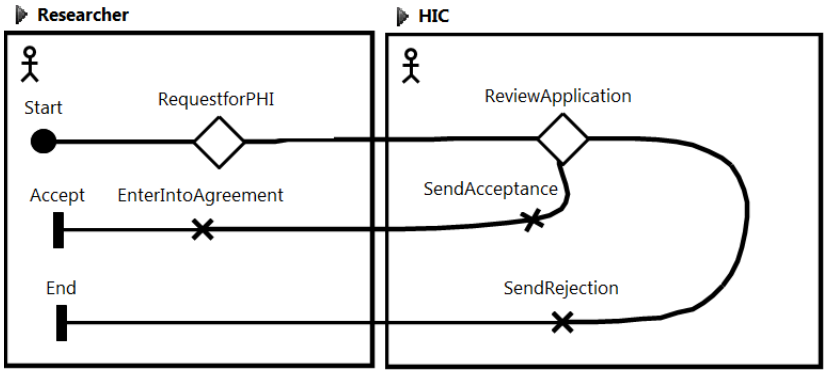

Figure 6.7: Top-Level UCM for PHIPA- Disclose to Researcher

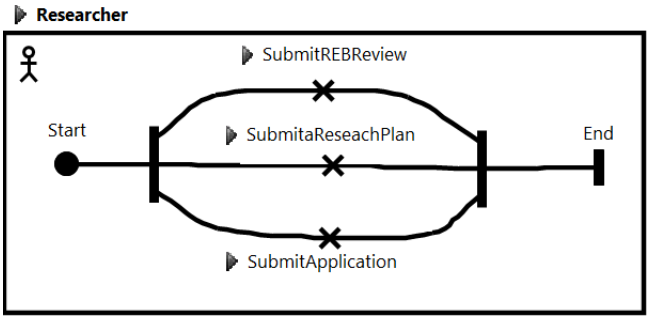

Figure 6.8: PHIPA UCM for Researcher

6.5 Step 6 – Developing Organizational GRL and UCM

In the organization model, the hospital has five high-level goals (modeled as softgoals): Provide Better Healthcare (PBH), Improve Quality of Services (IQS), Protect Privacy and Confidentiality of PHI (PPC), Increase Understanding of Public Health (IUPH), and Minimizing Cost (MC). The hospital ranks these softgoals based on their importance. The first three softgoals are of high importance for the hospital, therefore they get an importance value of 100 while the last two goals have an importance higher than medium but not as high as the first three. These two softgoals get an importance value of 75. These values are shown between parentheses for the softgoals in Figure 6.9.

In addition, the hospital has five main PHIPA-related goals that contribute to the five above softgoals: Disclose PHI to Researcher, Disclose PHI to Hospital Employees, Collect, Use or Disclose PHI to Obtain Payment, Collect, Use or Disclose PHI to Monitor, Verify or Reimburse Claim and Collect, Use or Disclose PHI to Investigate Breach. In our case study, we modeled each of these five goals in separate but related diagrams and we added contributions from these goals to five hospital softgoals shown in Figure 6.9 and Table 6.3.

Each of the goals of the hospital expands to lower-level activities and tasks. We modeled each of these goals and their low-level tasks in a separate GRL model.

In Figure 6.10, the goal model for the hospital Disclose PHI to Researcher is presented. The other two goal models are shown in Appendix D.

Table 6.3: Hospital Goals to Softgoals Contribution Values

	PBH	IQS	PPC	IUPH	MC
... PHI to Researcher	25	25	-25	50	10
... PHI to Hospital Employees	75	50	-25	50	10
... PHI to Obtain Payment	-	-	-25	-	30
... PHI to Monitor, ... Claim	-	-	-25	-	30
... PHI to Investigate Breach	-	25	100	-	20

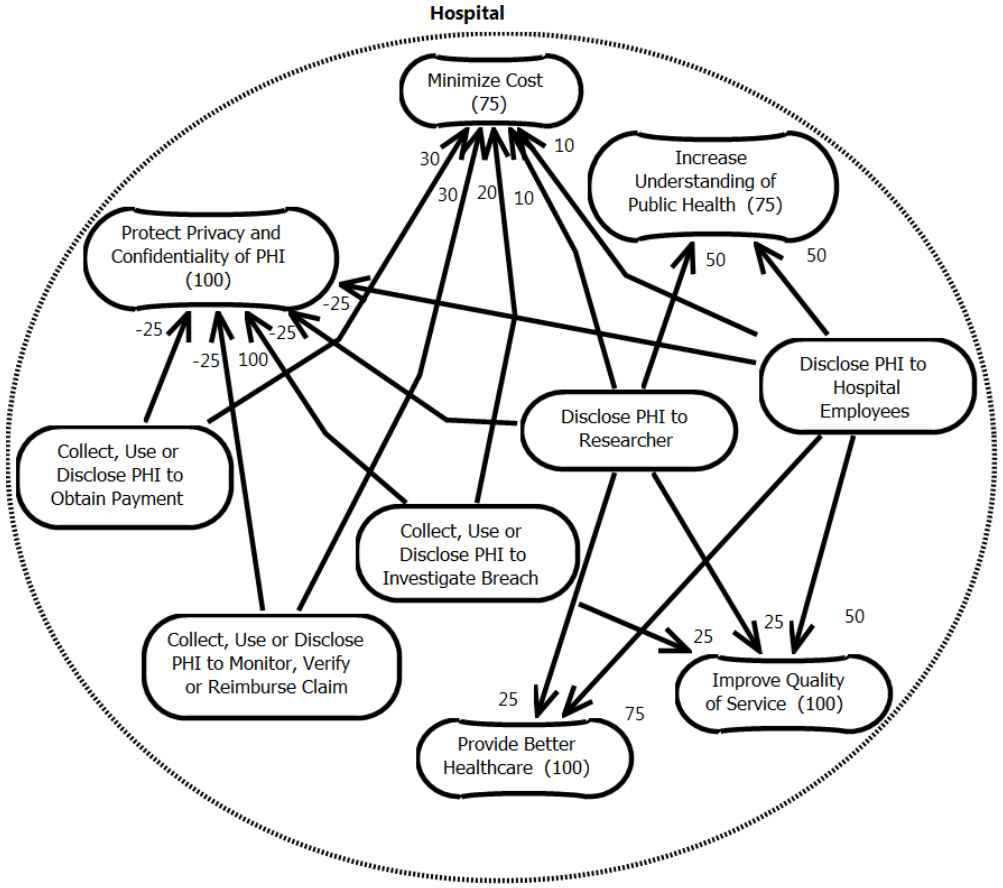

Figure 6.9: Hospital High-level Goal Model

The hospital discloses PHI to the external researcher who aims to perform research on new diseases. With this activity, the hospital contributes to all of its softgoals positively except the softgoal Protect Privacy and Confidentiality of PHI. If the hospital follows the privacy regulation (i.e., PHIPA), it can reduce this negative effect to a lower value (-25 here).

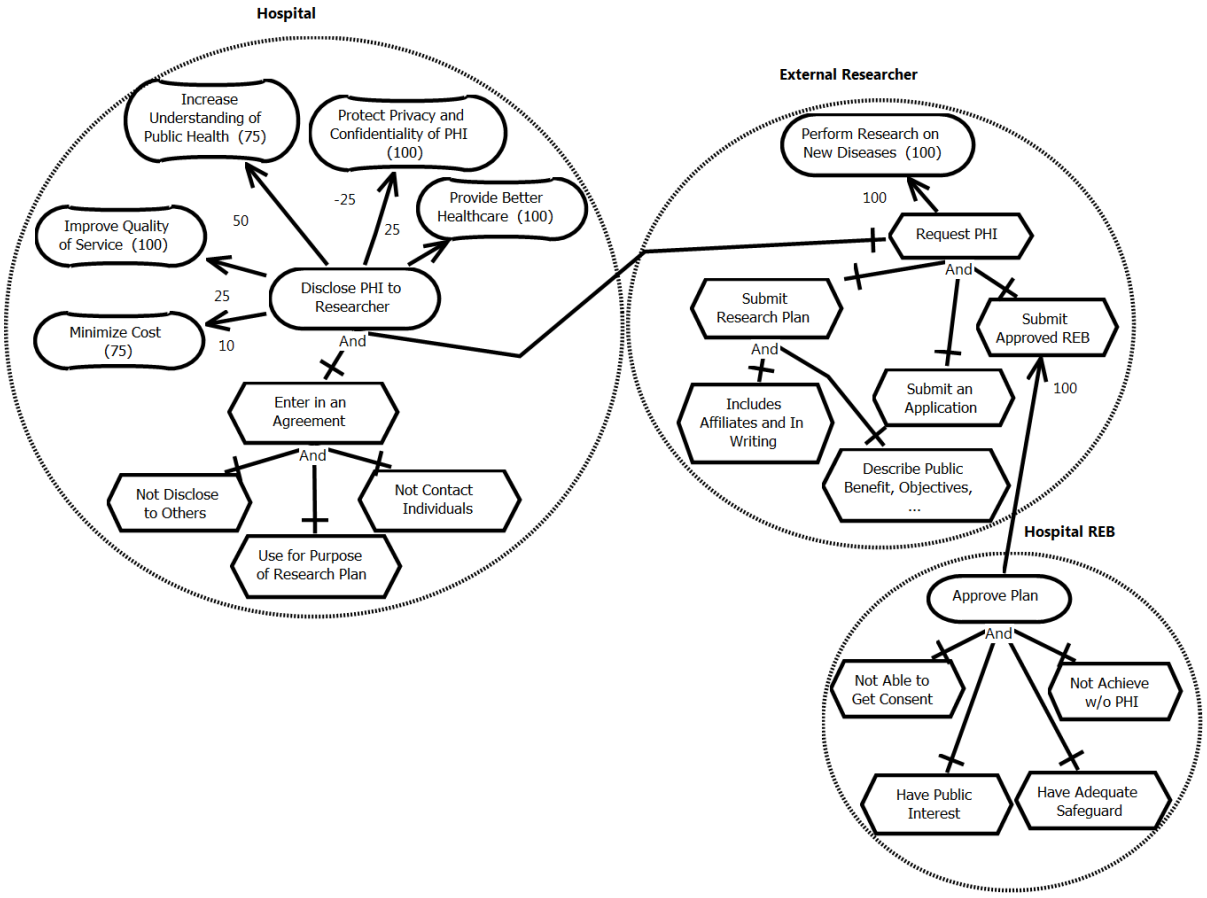

Figure 6.10: Hospital - Disclose PHI to Researcher Goal Model

External researchers need to access patient data (PHI or HI) to perform their research thoroughly. In order to provide access to PHI, the hospital asks the researcher to submit an application, submit a research plan in the correct format and submit the approval from the Research Ethics Board (REB). If the application of the researcher is completed and approved by the hospital, then the hospital signs an agreement with the researcher. The agreement outlines that the researcher is not allowed to disclose the PHI to others, is not allowed to contact the individual, and can only use the PHI for the purposes outlined in the research plan (see Figure 6.10 for details). Note that the conventional modeling of goals and tasks with GRL is used here, and details of these steps are discussed in the literature.

The hospital needs the REB approval for the research plan to be able to make its decision on whether to accept or deny the researcher's request. The REB has to consider several facts (shown in Figure 6.10) to approve the research plan.

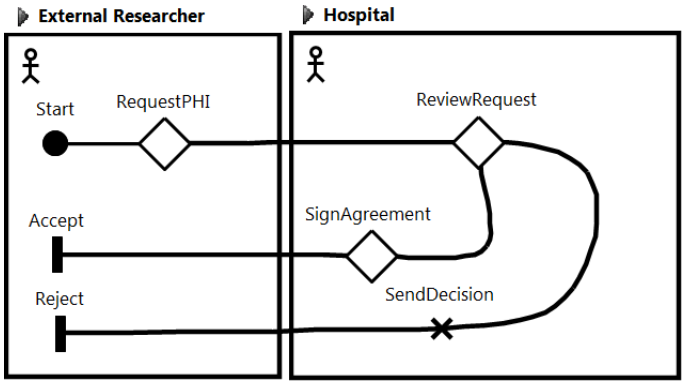

Figure 6.11: UCM RootMap for Disclose PHI to Researcher

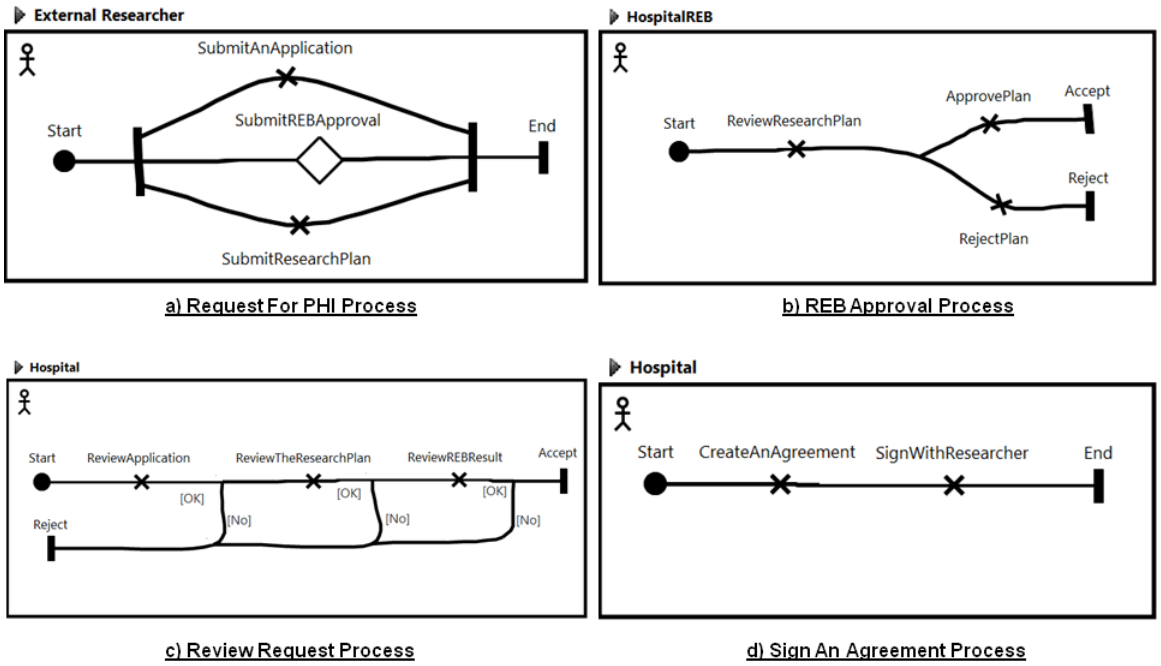

Figure 6.12: UCM Low-Level Processes for Disclose PHI to Researcher

Since the processes for the hospital, the researcher and the REB contain some sequential and parallel activities, we model the hospital business processes for disclosing

PHI to the external researcher with UCMs as well. Figures 6.11 and 6.12 illustrate the business process for disclosing PHI to researchers.

6.6 Step 7 – Defining Consequence Goals and Model

When the legal model was built, we identified three consequences of non-compliance as «Consequence» goals: Avoid Bad Reputation, Avoid Financial Penalties and Avoid Lawsuits. High-level goals of the legal model were connected to these consequence goals through contribution links, which define the importance of each legal goal on the related consequence goals. The links from the related legal model to the «Consequence» goals have positive contributions. If legal goals are fully achieved, then consequence goals get the value 0 (or "None") otherwise they get a value from -100 up to 0 (i.e., denied or weakly denied). Figure 6.13 presents the legal goal model of Article 29 (which shows the high-level goals for collect, use and disclosure) together with its consequence links.

To help in reading the model, we also hid the intentional elements that are not used in our case study or that have no links to the consequences. Note that we selected here equal values for the contributions from legal goals to consequence goals since we believed these goals are equally important in the law, and because their non-compliance has the same impact on the consequence goals. However, it is not necessary to have equivalent values for all of the contributions.

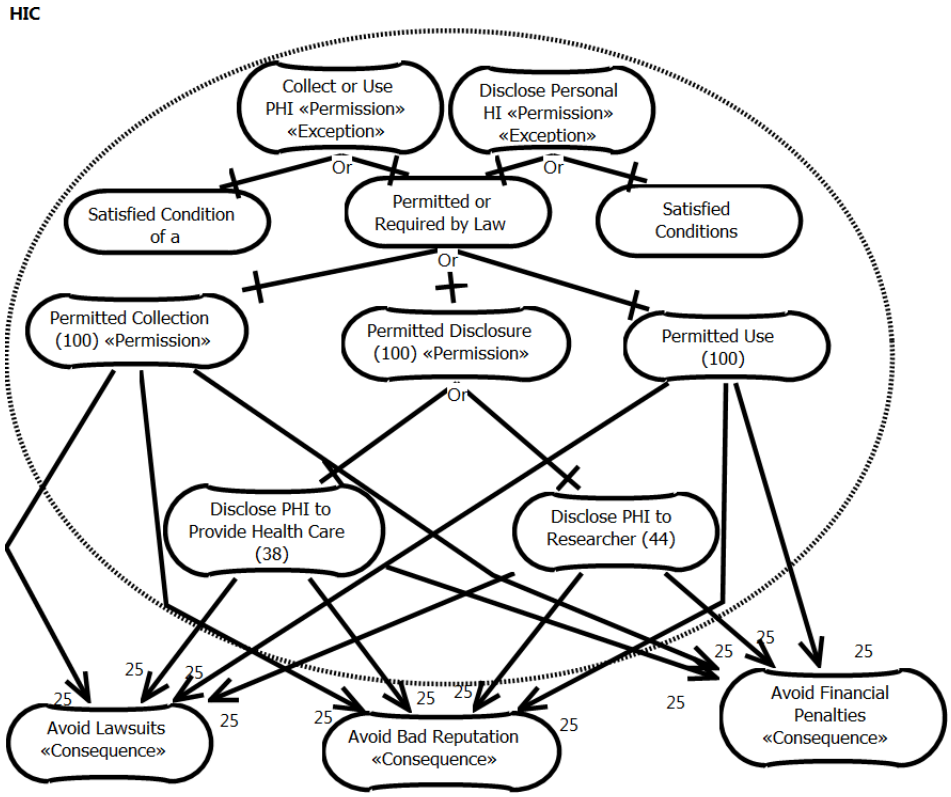

Figure 6.13: Consequence Graph

6.7 Step 8 – Establishing Framework Links

After both legal and organizational models are built, we connect elements of each model to their source documents through source links, GRL models to the Hohfeldian models (refer to Chapter 2) through compliance links, and finally UCM models to GRL models through responsibility links.

In this case study, since we aim to analyze the compliance and prioritize the instances of non-compliance, we mainly look at GRL models and the links between them. Furthermore, since UCM models are linked to GRL models, any non-compliance instance or potential improvement will be reflected in the business processes as well.

To set up the models, we also connect actors, tasks and goals of the hospital model to elements in the legal model through *weighted traceability* links and *simple traceability* links.

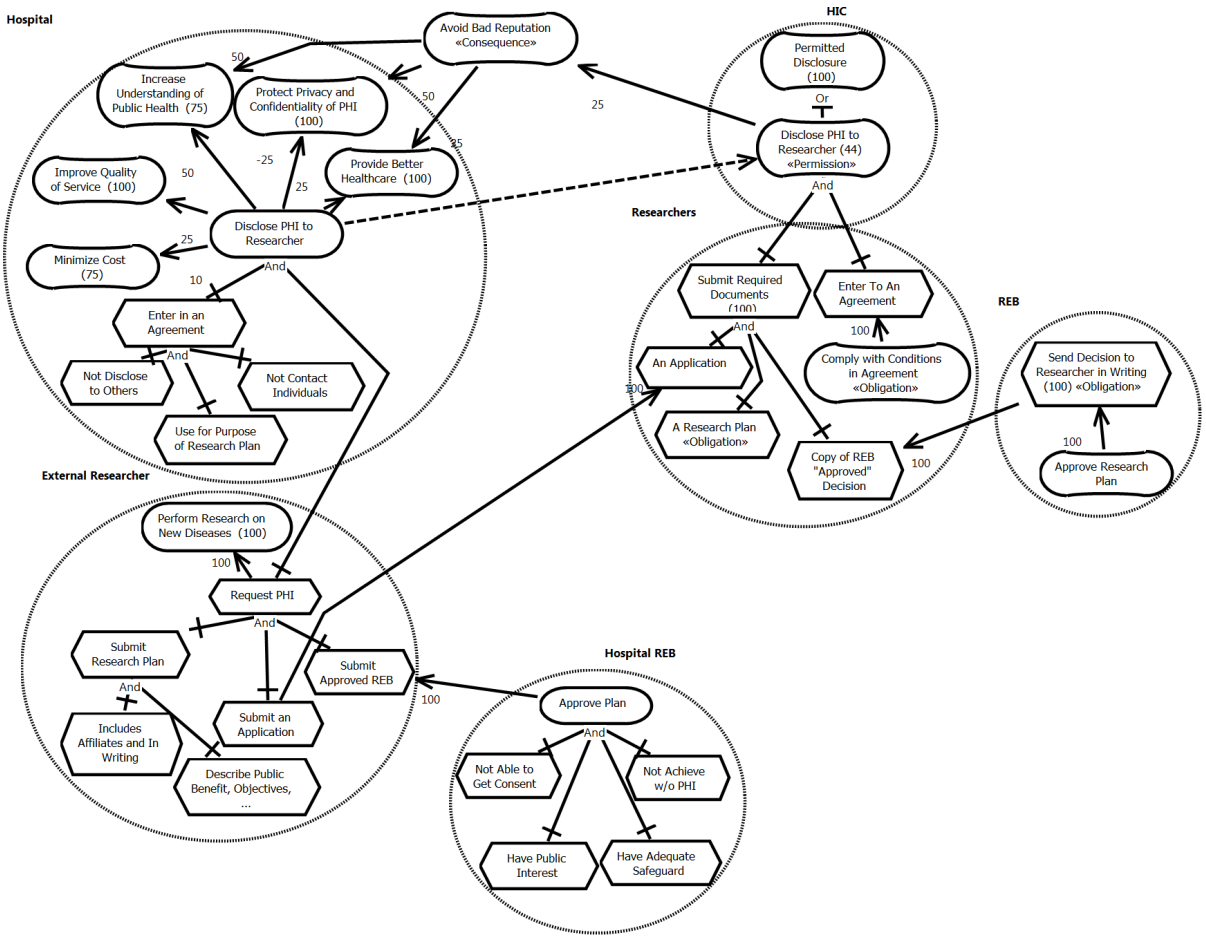

Figure 6.14: Organization GRL Model (Left) Linked to the Legal GRL Model (Right)

Furthermore, we add weighted «Consequence» links between consequence goals and softgoals in the hospital model.

Figure 6.14 shows only a partial view of the model (it only extends the goal for Disclose PHI to Researcher). There are four views for Disclose PHI to Researcher model and 5 other views for the other goals of the hospital. The whole model is composed of 11 actors (41 references), 99 intentional elements (244 references), 90 intentional links (199 references), 6 URN links, and 41 diagrams. The other five views of the hospital goals (i.e., Collect, Use or Disclose PHI to Healthcare Providers (Hospital Employees); Collect, Use or Disclose PHI for Payment or Reimbursement; and Collect, Use or Disclose PHI

for Investigating the Breach) are presented in Appendix D.

As shown in Figure 6.14, there is a *simple traceability* link between the goal Disclose PHI to Researcher of the hospital model and the goal Disclose of PHI to Researcher of the legal model. In addition, the low level tasks in the hospital model, have *weighted traceability* links to two tasks in the legal model, the low level tasks of the legal model (for example, Submit an Application to An Application, Not Disclose to Others to Not Disclose PHI, Use for Purpose of Research Plan to Use PHI for Purpose of Research Plan, and Not Contact Individuals to Not Contact Individual). The rest of the *weighted traceability* links can be found in Appendix D.

6.8 Compliance Analysis

After having created all the required models for our case study, we perform compliance analysis with respect to the steps identified in Chapter 5.

6.8.1 Steps A and B - Annotations and Links

In Step A, we annotate the intentional elements of the Legal GRL models that are not relevant to the context of the organization with «No». In this chapter, we have already identified the non-relevant parts of the law. «NoPreCondition» tags are inserted dynamically while running the quantitative or qualitative compliance analysis algorithms (and removed automatically after an evaluation).

Step B requires the annotation of the links with their relevant stereotype. In this chapter, this step occurred while establishing links between the two parts of the framework.

6.8.2 Step C - OCL Well-formedness Rules

Once the linked models are available, the jUCMNav tool is used to check the OCL well-formedness rules. After fixing a few small issues with tagging stereotypes properly, we

got the confirmation that all 18 rules passed, as shown in Figure 6.15.

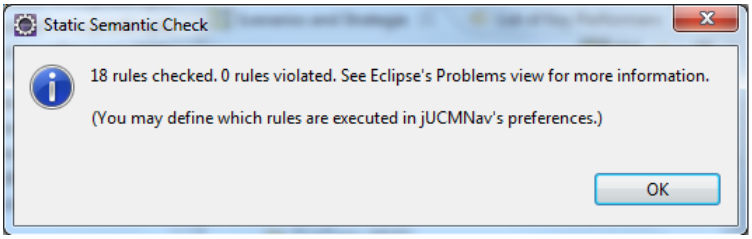

Figure 6.15: Result of Well-formedness Rules Checking

6.8.3 Step D - Quantitative and Qualitative Compliance Analysis (As-Is Strategy) – Bottom-Up Approach

In the previous section, we built the models and established links between goal models and business processes. However, we did not cover all of the business processes of the hospital. We only focused on the case study related to disclosing PHI to the researcher since it is one of the main issues of the hospital. In this section, first we select a base strategy and illustrate the qualitative and quantitative compliance analysis techniques and examine the degree of compliance of our organization to PHIPA. Then, we present the effect of these analyses on the business processes.

Quantitative Analysis of Goal Models

In this case study, we analyzed the organizational model quantitatively. As mentioned before, qualitative analysis is used when there is little information about the satisfaction values or the contribution links whereas quantitative analysis is used when more precise data is available.

For this example, we assume that the hospital performs most of its tasks completely and therefore the quantitative value 100 is assigned to them. These tasks are Submit an Application, Not Able to Get Consent, Not Achieve w/o PHI, Have Public Interest, Proceed with Claims, Proceed with Payment, Investigate Researcher Breach, Not Able to Collect,

Disclose Accurate Information, Unable to Get Direct Consent In Time, Analyze a New Disease, Includes Affiliates and In Writing, and Describe Public Benefit, Objectives, ... The hospital also provides some safeguards, leading to a satisfaction of 50 for the task Have Adequate Safeguard. Through decomposition and contribution links in the organization GRL model, these initial values propagate to the higher-level goals and softgoals of the organization. In Figure 6.16, we expand the goal Disclose PHI to Researcher.

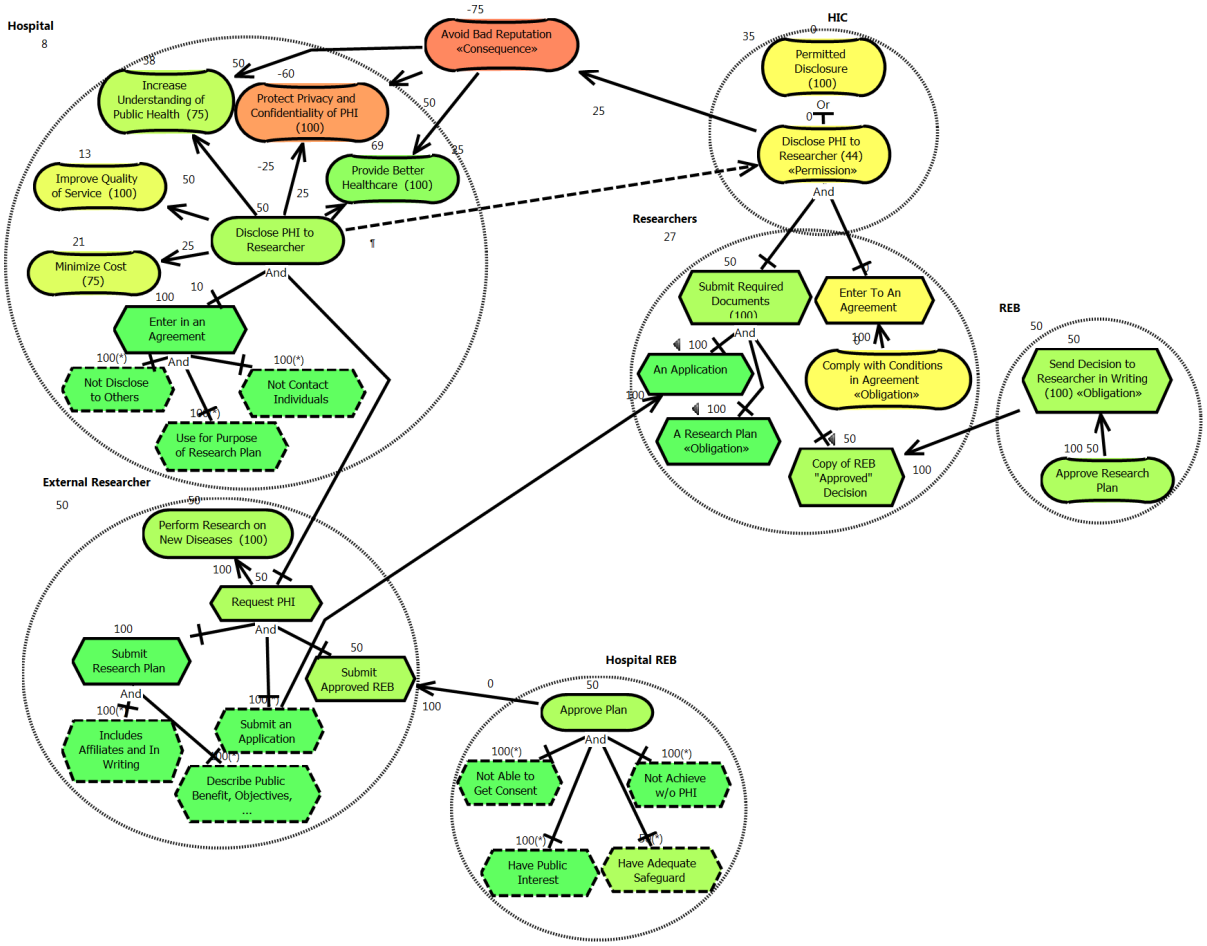

Figure 6.16: Quantitative Analysis of Base Strategy

Using the propagation algorithm, the goals Disclose PHI to Hospital Employees, Collect, Use or Disclose PHI to Investigate Breach, Collect, Use or Disclose PHI to Monitor, Verify or Reimburse Claim and Collect, Use or Disclose PHI to Obtain Payment of the hospital get

the value 100 and the goal Disclose PHI to Researcher get the value 50.

Values for contribution links of both models and the *weighted traceability* links are defined based on the importance and the effect of each task on intentional elements related to it, from the hospital and legal points of view. These values propagate to the higher-level intentional elements of the organizational model via contribution and decomposition links, and to the legal model through *weighted traceability* links. Figure 6.16 shows only one view out of the 9 views capturing the whole model. However, the compliance analysis is for the whole model.

As shown in the figure, the task Submit Required Documents in the legal model has a satisfaction level of 50 while the task Enter To An Agreement in the legal model evaluates to 0. The task Submit Required Documents has three subtasks: Submit an Application and Submit Approved REB with links to tasks in organizational model get a 100 value whereas the task Copy of REB "Approved" Decision gets 50, similar to the value of the task Submit Approved REB in the organizational model. These values propagate to the higher levels also via contribution and decomposition links. As a result, the obligation goal Disclose PHI to Researcher (44) and Permitted Disclosure get a 0 satisfaction value. The same process is followed for the other tasks related to the other goals of the hospital model. Since all of the tasks related to the legal goal Permitted Use have the value 100, this goal also gets 100. However, since some of the tasks related to the goal Permitted Collection are not satisfied and some tasks are missing in the organizational model, this goal gets a 0 value. Finally, since some of the goals bound to the HIC actor have a 0 value and one has 100, this actor gets the satisfaction value 35.

Note that, in this quantitative analysis, the legal goals with «No» tags are omitted from the analysis and are shown with *gray* color (see Figure D.16)

Note also that two of the legal goals do not have a value higher than 0, and that the consequence goals get the value -75. These consequence goals also have some effect on the organization's softgoals. In Figure 6.16, these values are illustrated. We observe that none of the softgoals of the organization have a 100 satisfaction value: Provide

Better Healthcare = 69, Increase Understanding of Public Health = 38, Minimize Cost = 21, Improve Quality of Service = 13 and Protect Privacy and Confidentiality of PHI = −60 . As a result, the Hospital actor's satisfaction value is 8.

The other 8 views are presented in Appendix D.

Qualitative Analysis of Goal Models

We also used the qualitative analysis algorithm to perform the same study. The objective here is to demonstrate that this second algorithm has also been implemented properly. Choosing between the two algorithms should be based on the availability of sufficient knowledge about the organization; the quantitative algorithm should be used only when good knowledge is available otherwise improper numerical contribution numbers may lead to incorrect conclusions.

We select tasks that the hospital performs to reach its own goals while complying with PHIPA at the same time. As in the previous analysis, all of the basic tasks get *Satisfied* as a qualitative satisfaction, except for task Have Adequate Safeguard, which initialized to *Weakly Satisfied*. Through decomposition and contribution links in the organization GRL model, these initial values propagate to the higher-level goals and softgoals of the organization. In Figure 6.17 and Figure 6.18, we present two other views of the model that focus on the organization goal Collect, Use or Disclose PHI to Investigate Breach.

As in the quantitative analysis example, the organizational goals are *Satisfied*, except for Disclose PHI to Researcher (*Weakly Satisfied*).

Since the organizational tasks are also connected to the legal model's tasks through *weighted traceability* links, their satisfaction values propagate to the legal tasks. Figure 6.17 and Figure 6.18 show the result of this analysis. The task Investigating Breach in the legal model is *Satisfied* while the task HIC is an Institution within Meaning of FIPPA or MFIPPA in the legal model gets the value *None*. This task refers to another regulation, i.e., FIPPA or MFIPPA. Since Legal Agency is not under the definition of permitted institutions, this task is not satisfied. These values also propagate to higher level goals

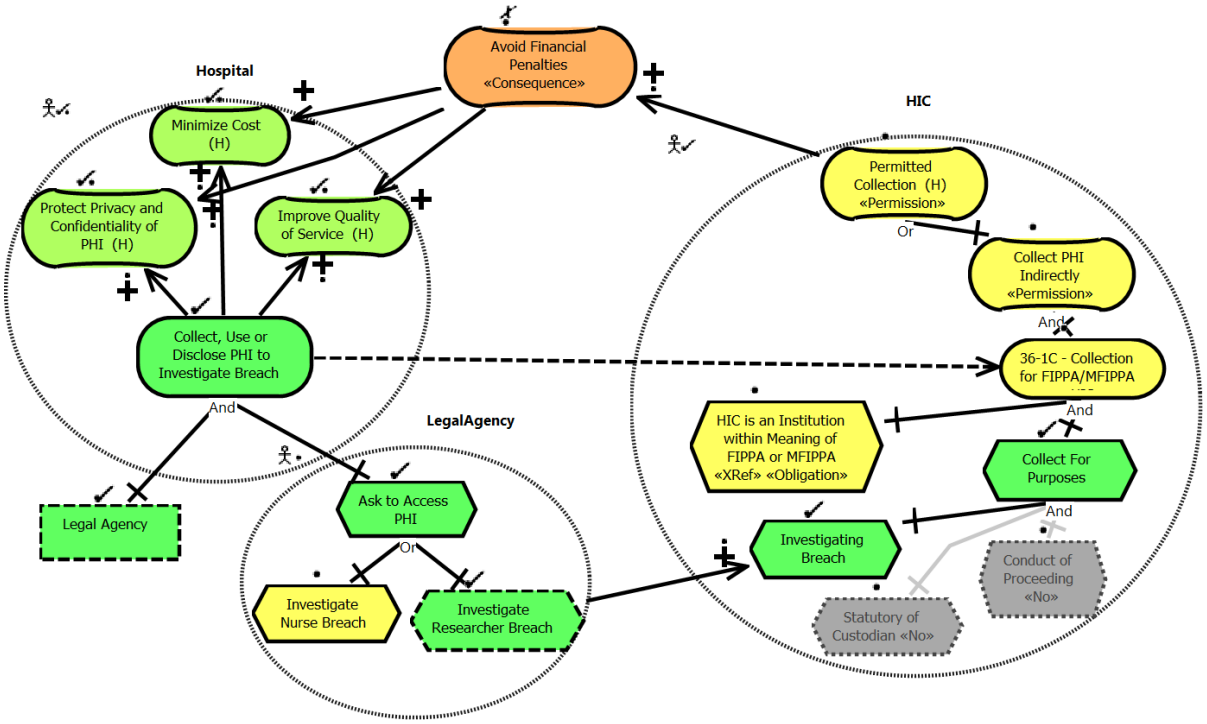

Figure 6.17: Qualitative Analysis of Base Strategy - View 1

via contribution and decomposition links. As a result, the permission softgoal Permitted Collection gets a *None* satisfaction value. The same process is followed for the other tasks related to the other goals of the hospital model (7 other views). Similar to the quantitative analysis, all of the tasks related to the legal goal Permitted Use are satisfied, thus, this goal is *Satisfied*. However, some of the tasks related to the goal Permitted Disclosure are not satisfied. Therefore, this goal gets a *None* value. Finally, since some of the goals bound to the HIC actor have a *None* value and one has *Weakly Satisfied*, this actor gets the satisfaction value *Weekly Satisfied*.

Each legal goal is connected to the consequence goals via contribution links. Two out of three softgoals of the legal model have a satisfaction value not higher than *None*. This results in consequence goals with satisfaction value *Weakly Denied*. These consequence goals also have some effect on the organization's softgoals. In Figure 6.17, these values are illustrated. As it is shown, all of the softgoals of the organization get the value

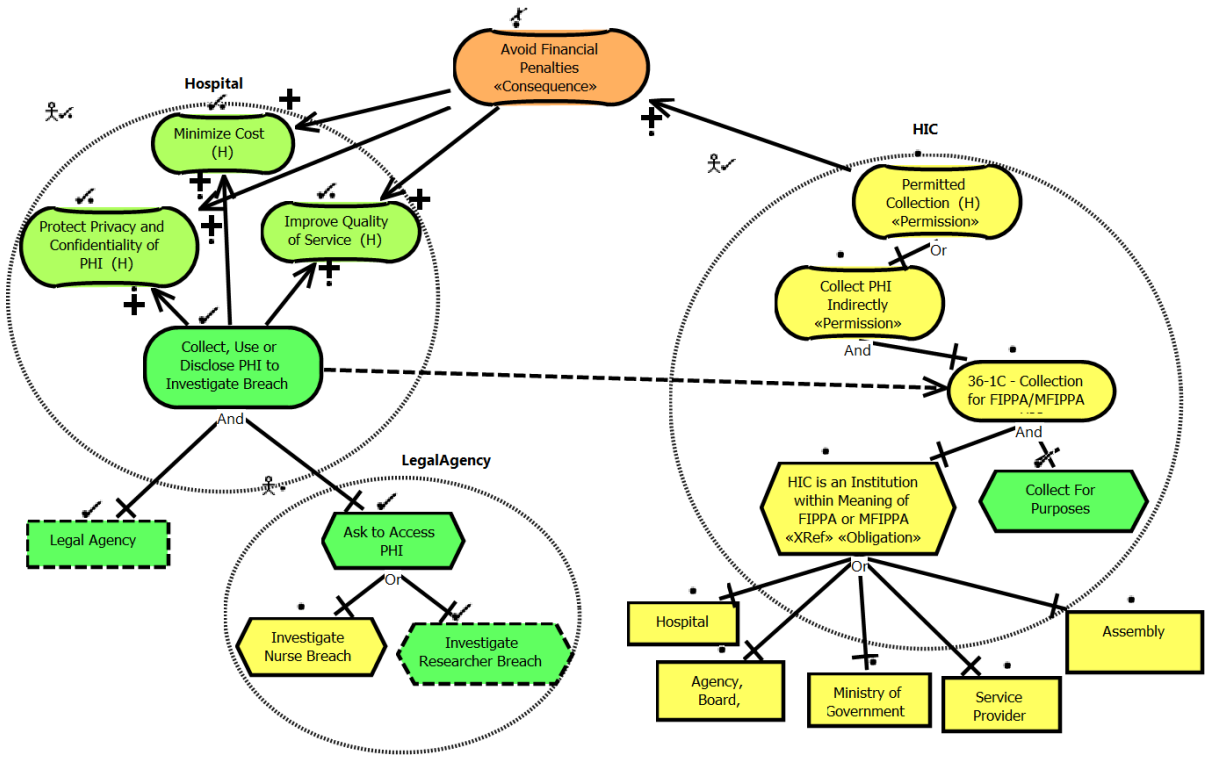

Figure 6.18: Qualitative Analysis of Base Strategy - View 2

Weakly Satisfied. For this reason, the satisfaction value of the actor Hospital is also *Weakly Satisfied*.

Effect of the GRL Model on the Business Processes of the Law and Organization

As mentioned in Section 4.7.4), different elements of a Use Case Map (i.e., components, responsibilities and stubs) are linked to their corresponding elements in the GRL view (i.e., actors, goals and tasks). In this way, the satisfaction levels of the UCM elements are determined by the satisfaction values of their linked GRL elements. These numbers help us to identify responsibilities, sub-processes and components in the business process that do not have a satisfaction value of 100 and that, therefore, need improvement.

In Figure 6.19, HIC and Researcher get satisfaction values of 35 and 27 respectively

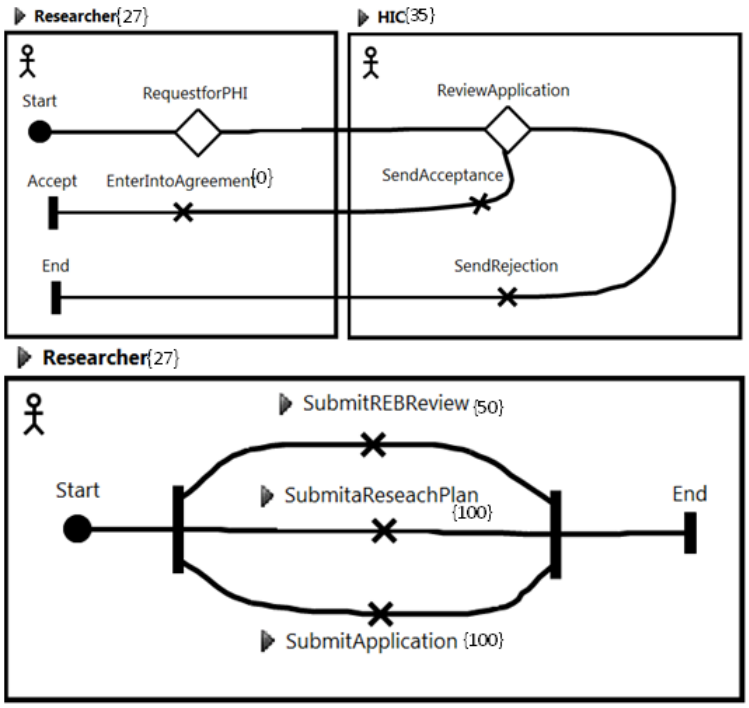

Figure 6.19: Business Process Compliance Analysis

based on the value of their corresponding actors in the GRL model. This indicates that the business process of the hospital is not compliant with PHIPA. After analyzing the elements of the business process, it becomes obvious that the responsibilities EnterIntoAgreement and SubmitREBReview, with 0 and 50 as respective values, are two activities that are missing/incomplete in the hospital's business process. Therefore, it is necessary to modify the hospital business process so that it complies with PHIPA and its objectives and procedures.

6.8.4 Step E - OCL Compliance Rules Checking

After having developed strategies (Section 6.8.3) and calculated the degree of compliance of the organizational model to the legal model, we check the OCL compliance rules explained in Chapter 5 against the model. Figure 6.20 shows the feedback provided by the tool, with the numbers of rules checked (5) and violated (2 in this case). In order to

identify which rules are violated, the analyst can use jUCMNav's Problems view. The results, shown in Figure 6.21, indicate that the two rules were violated numerous times, for a total of 13 warnings due to non-compliance instances. Such violations need to be resolved.

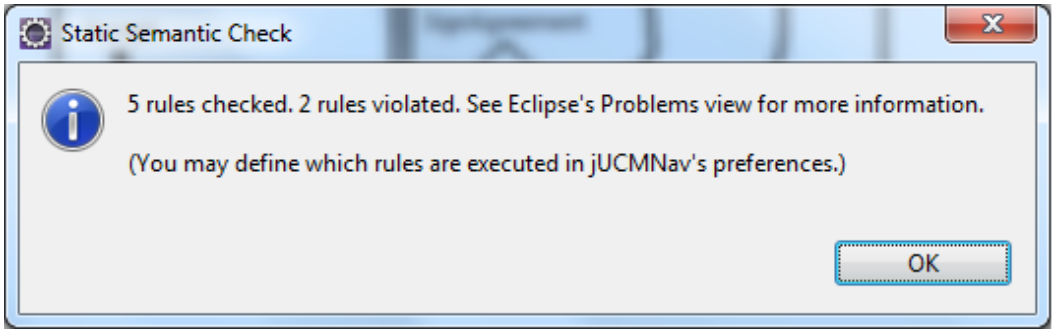

Figure 6.20: Number of Violated Rules

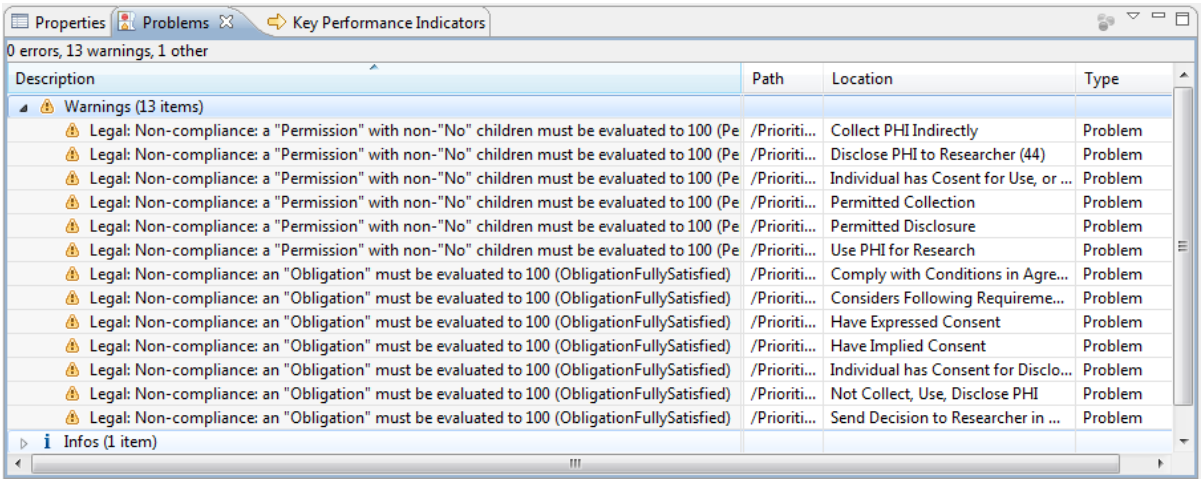

Figure 6.21: OCL Compliance Rules Result

In the example, 6 out of the 13 violations are related to rule 20 and the other 7 violations are related to rule 19. For example, the first violated rule in the list is related to rule 20 and it is located at goal "Collect PHI Indirectly" (the analyst can simply double-click on the violation, and the tool will bring the relevant diagram and violating object from the model). This rule indicates that the "Permission" goal with non-"No"

children must be evaluated to 100. However, as shown in figure 6.18, this goal is evaluated only to 0. Thus, this rule is violated in the location of the goal 'Collect PHI Indirectly".

Knowledge about these violations is at the basis of the approach to establish an appropriate strategy for improving the compliance level of the organization.

6.8.5 Steps F and G - What-If Strategies and Prioritization Algorithm

In the previous section, we analyzed the compliance of the hospital model against PHIPA and discovered non-compliant instances. We identify 5 undecomposed tasks with a value of less than 100: (a) Have Adequate Safeguards, (b) Comply with REB Conditions, (c) Notify Breach, (d) Not Publish PHI in a Form That Makes it Identifiable, and (e) HIC is an Institution within Meaning of FIPPA or MFIPPA.

To prioritize these tasks, we follow the steps discussed in Section 5.6. We generate a strategy for each combination of 0 or 100 satisfaction value for each of the tasks. As we have 5 tasks here, this leads to $2^5 = 32$ strategies. For each strategy, we calculate satisfaction levels for all actors (Hospital and HIC here), providing values for OrgPr and LegalPr. We then compute the priority value of each strategy based on the formula defined in Section 5.6.2.

In this example, we believe that satisfying The Ontario Hospital and satisfying PHIPA are equally important, and slightly more important than the complexity of legal requirements implementation. We hence give equal weights of 0.35 for ω_1 and ω_2, and 0.30 for ω_3. In addition, since the missing tasks are somewhat equally complex according to the evaluation of their legal text (as described by Massey et al. [72]), we set the complexity value of each strategy based on the number of tasks initialized at 100. Hence, the strategy with no task gets the complexity value ComPr = 100, strategies with only one task get 80, etc. The fewer tasks needed, the higher the priority factor based on complexity.

The result of this analysis is shown in Table 6.4. In columns a to e, we indicate which

tasks have been selected for the corresponding strategy. According to these results, the best strategy is Strategy 6, which covers (e) HIC is an Institution within Meaning of FIPPA or MFIPPA. Assuming that this task e is implemented, the next best strategy is Strategy 10 with an additional task (a) Have Adequate Safeguards. Then, assuming that tasks a and e, have been implemented, Strategies 19, 20 and 22 (with the same priority value: 46.3) and three tasks (b, c, and d) are the best ones following Strategies 6 and 10.

Once this step is completed, the evolution path for this organization to achieve full legal compliance can be determined. The hospital first needs to make sure not to disclose PHI to an organization which does not fall into the category defined by FIPPA or MFIPPA, and then it needs to implement better safeguards. Next, the hospital has to implement a process to improve the agreement between the hospital and the researcher so that it ensures that the researcher will notify the breach, will not publish PHI in an identifiable way, and will comply with REB conditions, in any order.

Note that such evolution path is not solely based on the Priority column in Table 6.4. For example, Strategies 13, 15 and 16 have a priority score higher than that of Strategies 19, 20 and 22. However, Strategies 13, 15 and 16 are irrelevant in a context where tasks a and e have already been implemented (as they do not include task a).

6.8.6 Evaluation of Prioritization Algorithm

Let us assume that, after getting the results from the prioritization algorithm, we implemented support for the first suggested task ((e) HIC is an Institution within Meaning of FIPPA or MFIPPA) in the hospital's business process. jUCMNav can again be used to quantitatively analyze the compliance of the model after this change. Figure 6.22 shows the results of this analysis for the goal Collect, Use or Disclose PHI to Investigate Breach. The softgoal Permitted Collection of the legal model is now 100 compared to 0 in Figure D.16 (previous base strategy, quantitative evaluation). In addition, the value of the consequence goal improved from -75 to -50. This further results in improvements to the high-level goals of the hospital (from 8 to 27) and of the HIC's legal goals (from

Table 6.4: Priority Values for Each Strategy Evaluated

	a	b	c	d	e	W1	OrgPr	W2	LegalPr	W3	CompPr	Priority
Strategy 1						0.35	8	0.35	35	0.3	100	45.05
Strategy 2	X					0.35	14	0.35	35	0.3	80	41.15
Strategy 3		X				0.35	8	0.35	35	0.3	80	39.05
Strategy 4			X			0.35	8	0.35	35	0.3	80	39.05
Strategy 5				X		0.35	8	0.35	35	0.3	80	39.05
Strategy 6					X	0.35	27	0.35	65	0.3	80	56.2
Strategy 7	X	X				0.35	14	0.35	35	0.3	60	35.15
Strategy 8	X		X			0.35	14	0.35	35	0.3	60	35.15
Strategy 9	X			X		0.35	14	0.35	35	0.3	60	35.15
Strategy 10	X				X	0.35	33	0.35	65	0.3	60	52.3
Strategy 11		X	X			0.35	8	0.35	35	0.3	60	33.05
Strategy 12		X		X		0.35	8	0.35	35	0.3	60	33.05
Strategy 13		X			X	0.35	27	0.35	65	0.3	60	50.2
Strategy 14			X	X		0.35	8	0.35	35	0.3	60	33.05
Strategy 15			X		X	0.35	27	0.35	65	0.3	60	50.2
Strategy 16				X	X	0.35	27	0.35	65	0.3	60	50.2
Strategy 17	X	X	X			0.35	14	0.35	35	0.3	40	29.15
Strategy 18	X	X		X		0.35	14	0.35	35	0.3	40	29.15
Strategy 19	X	X			X	0.35	33	0.35	65	0.3	40	46.3
Strategy 20	X		X		X	0.35	33	0.35	65	0.3	40	46.3
Strategy 21	X		X	X		0.35	14	0.35	35	0.3	40	29.15
Strategy 22	X			X	X	0.35	33	0.35	65	0.3	40	46.3
Strategy 23		X	X	X		0.35	18	0.35	52	0.3	40	36.5
Strategy 24		X	X		X	0.35	27	0.35	65	0.3	40	44.2
Strategy 25		X		X	X	0.35	27	0.35	65	0.3	40	44.2
Strategy 26			X	X	X	0.35	27	0.35	65	0.3	40	44.2
Strategy 27	X	X	X	X		0.35	33	0.35	70	0.3	20	42.05
Strategy 28	X	X	X		X	0.35	33	0.35	65	0.3	20	40.3
Strategy 29	X	X		X	X	0.35	33	0.35	65	0.3	20	40.3
Strategy 30	X		X	X	X	0.35	33	0.35	65	0.3	20	40.3
Strategy 31		X	X	X	X	0.35	37	0.35	82	0.3	20	47.65
Strategy 32	X	X	X	X	X	0.35	54	0.35	100	0.3	0	53.9

35 to 65). Table 6.5 provides a comparison between the base strategy and Strategy 6 for the hospital's high-level goals.

When we run the OCL compliance rules, we also get some improvement. The number

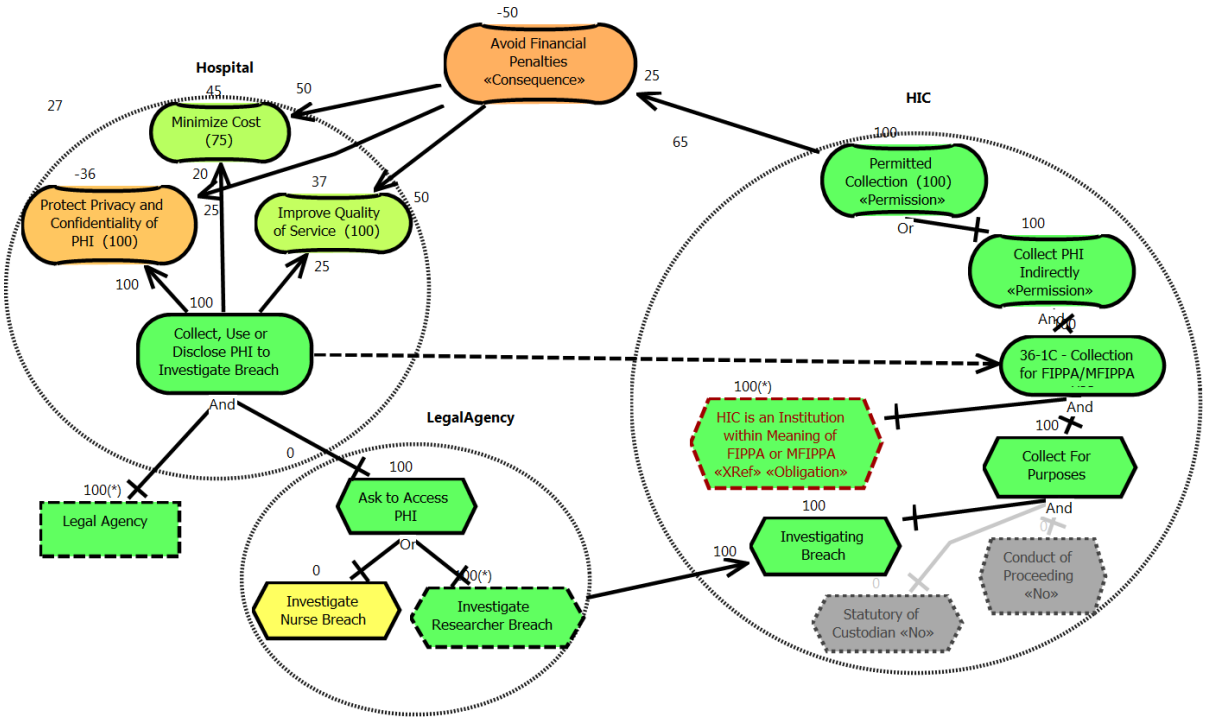

Figure 6.22: Quantitative Analysis - Task E Implemented

Table 6.5: Hospital Softgoals Satisfaction Values - Comparison

	PBH	**IQS**	**PPC**	**IUPH**	**MC**
Base Strategy	69	13	-60	38	21
Strategy 6 Implemented	75	37	-36	50	45

of warnings decreases from 13 to 9 (Figure 6.23) when compared to the situation with the base strategy.

After implementing task e, we remain with 4 non-compliant instances. Based on the prioritization algorithm, we have $2^4 = 16$ strategies. We repeat the steps of Section 6.8.5 for these 16 strategies to validate the path we suggested in the previous section.

As the weights remain unchanged, we still have 0.35 for ω_1 and ω_2, and 0.30 for ω_3. The complexity value ComPr is now going from 100 (simplest) down to 0 by increments of -25. Hence, the strategy that implements task e only (i.e., the new baseline) gets the value 100 and the strategy that implements all of the four tasks gets 0. Table 6.6

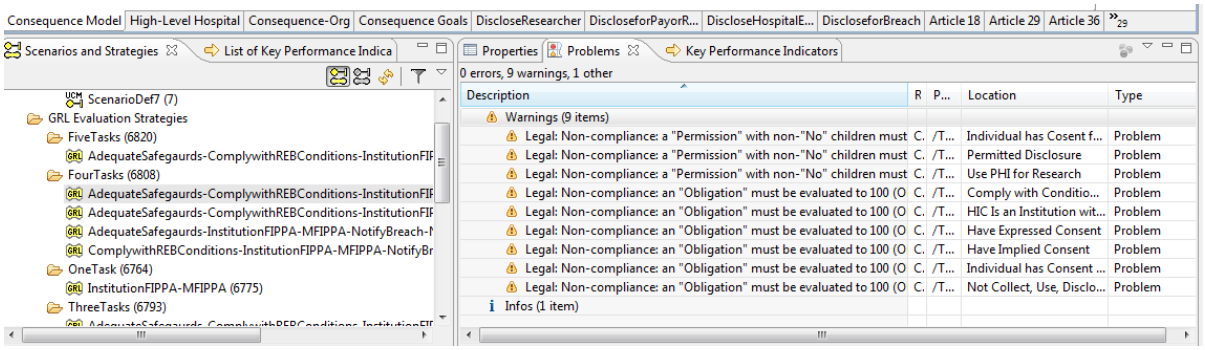

Figure 6.23: OCL Compliance Rules Results - Task E Implemented

illustrates the results of the prioritization algorithm for all 16 strategies. Note that in all of these strategies, task e is implemented.

Table 6.6: Priority Values for Each New Strategy Evaluated After Implementing Task E

	a	b	c	d	e	W1	OrgPr	W2	LegalPr	W3	CompPr	Priority
Strategy 1					X	0.35	27	0.35	65	0.3	100	62.2
Strategy 2	X				X	0.35	33	0.35	65	0.3	75	56.8
Strategy 3		X			X	0.35	27	0.35	65	0.3	75	54.7
Strategy 4			X		X	0.35	27	0.35	65	0.3	75	54.7
Strategy 5				X	X	0.35	27	0.35	65	0.3	75	54.7
Strategy 6	X	X			X	0.35	33	0.35	65	0.3	50	49.3
Strategy 7	X		X		X	0.35	33	0.35	65	0.3	50	49.3
Strategy 8	X			X	X	0.35	33	0.35	65	0.3	50	49.3
Strategy 9		X	X		X	0.35	27	0.35	65	0.3	50	47.2
Strategy 10		X		X	X	0.35	27	0.35	65	0.3	50	47.2
Strategy 11			X	X	X	0.35	27	0.35	65	0.3	50	47.2
Strategy 12	X	X	X		X	0.35	33	0.35	65	0.3	25	41.8
Strategy 13	X	X		X	X	0.35	33	0.35	65	0.3	25	41.8
Strategy 14	X		X	X	X	0.35	33	0.35	65	0.3	25	41.8
Strategy 15		X	X	X	X	0.35	37	0.35	82	0.3	25	49.15
Strategy 16	X	X	X	X	X	0.35	54	0.35	100	0.3	0	53.9

The table still gives the same result as the Table 6.4. The second best strategy is the one where a is done next (new Strategy 2), which includes task a. Among strategies with 3 tasks (that include tasks a and e), new Strategies 6, 7 and 8 (similar to the old

Strategies 19, 20 and 22), all with 49.3 priority values, are the next ones to consider, in any order.

This section demonstrates that the prioritization algorithm needs to be only done once and that the path given based on the algorithm remains the same if we repeat it again after implementing some of the tasks (assuming that no other change to the models occurred in the meantime).

6.9 Lesson Learned

We were able to use and validate the LEGAL-URN framework against a case study related to compliance of The Ontario Hospital with the PHIPA law. With this framework, we were able to identify the Hohfeldian statements in PHIPA, model PHIPA with a Legal GRL/UCM model, and connect it to the organizational GRL/UCM model. With the help of OCL rules, qualitative/quantitative compliance analysis algorithms and a prioritization method based on what-if strategies, we ensured that the models are well-formed, we were able to systematically identify five non-compliant instances, and we provided a rigorous path for the organization to reach compliance.

Although this case study demonstrates the applicability of the framework to a particular situation, there are a few observable limitations. First, the resulting recommendations were not actually implemented in a real organization, so we cannot claim that they truly helped the organization reach a higher level of compliance. Second, even in this fairly realistic and sizable case study, we ended up with a limited number of tasks to select or not select in strategies, and so exploring all strategies was easy to do (and can be automated as well). However, as the number of strategies grows with the square of the number of tasks to select, this may not always be the case in other situations, and hence the relief solutions proposed in Section 5.6 might have to be explored further in the future. Third, we had only one law to handle here, whereas organization usually have to comply with many laws and regulations.

6.10 Summary

In this chapter, we provided our first case study, which was related to compliance with PHIPA. First, we presented an overview of the case study and then we went through the steps to build the model and verify its well-formedness. Next, we illustrated the quantitative and qualitative compliance analysis and identified the non-compliant instances through OCL compliance rules. Finally, we prioritized the non-compliance instances via our prioritization algorithm, and provided recommendations on where to start to improve compliance in the context of that organization. This was further validated by checking that the implementation of the first thing to do actually leads to compliance improvements, and that the rest of the path to full compliance remains the same.

The next chapter will address the third limitation mentioned in the previous section by looking at how best to handle multiple regulations.

Chapter 7

Handling Multiple Regulations

In previous chapters, we described how to build Legal-URN models for one single regulation, and how to use our tool-supported algorithms to analyze compliance and prioritize non-compliant instances in an organization. However, most organizations need to comply with more than one regulation at the same time. These different regulations can enforce exactly the same rules or have some overlap (e.g., one can be more detailed than the other). They can even conflict with each other. Also, one regulation can give a permission to perform an action whereas the same action in another regulation might be an obligation or an interdiction. In all of these cases, an organization needs to take different strategies.

In this chapter, we extend our framework to be able to capture more than one regulation, analyze the challenges in handling multiple regulations, and identify solutions for handling them. For this, first we provide an additional and specific literature review on existing relevant methodologies (Section 7.1). In Section 7.2, we define the high-level steps needed for comparing regulations as well as an extension of the Hohfeldian meta-model. Finally, in Section 7.3, we describe the pairwise comparison of each pair of statements and provide solutions for modeling them. This approach will be further illustrated and validated in the next chapter.

7.1 Handling Multiple Regulations: Related Work

Handling multiple regulations, being compliant with more than one regulation at the same time, and resolving conflicts between multiple regulations are challenging concepts for both researchers and organizations. In the last few decades, much work has been done to resolve conflicts in software requirements [22, 21, 89, 107]. However, up to now, very little work has been done to address these issues for the legal requirements domain.

Maxwell et al. [73] are amongst the first to provide a set of techniques to help requirements engineers identify, analyze and resolve conflicts in multiple regulations. This work identifies four patterns for internal and external cross-references. However, the main focus of this research is on two of the patterns, which are (i) external cross-references and (ii) internal cross-references that point to other portions of the legal text. With respect to these patterns, a legal cross-reference taxonomy is developed that consists of six categories: constraint, exception, definition, unrelated, incorrect, and general. This taxonomy is used to identify the type of conflicts caused by cross-references. Finally, after identifying the conflicts, based on a set of heuristics for identifying goal conflicts [107], the authors provide some guidance for their resolution. Although this work provides some grounds for identifying different cases when comparing multiple regulations, it mainly focuses on the conflicts caused by cross-references and not on comparing multiple regulations. In addition, this work only deals with textual requirements and not more abstract goal models.

Gordon et al. [33, 34, 35] introduced a framework that uses requirements watermarking and the requirements specification language (RSL) to (i) put high-level and low-level watermark standards across multiple regulations, (ii) translate the regulations to a canonical form and a set of statement and phrase-level metrics ([10]), and (iii) rationalize and analyze the differences and similarities between statements. In the watermarking framework, the first step is to extract and encode requirements from the two regulations with the RSL methodology (both manually and with tool support). The second step is to

compare the specifications, identify similarities and differences and measure the differences. Finally, the last step is to generate watermarks by identifying union disjoint and minimum watermarks.

RSL, which is used for the first step, contains a set of reserved keywords, special operators and line numbers to index different parts of a legal statement. These keywords are DOCUMENT, SCHEMA, and TITLE, respectively to capture a unique index for the regulation, the style of the document and its title; SECTION and PAR for section and all the paragraphs in the section; REFINE,EXCEPT and FOLLOWS to define the relations and cross-references; and finally INCLUDE, EXTERNAL, and EXEMPT for definitions and exemptions. There are operators such as "||" and "&" for logical-or and logical-and, and "!" for roles. RSL also captures modal verbs to illustrates the modality of a statement. To be able to perform the comparison, a set of metrics including *Near Equivalent, Pure Equivalent, Generalized Concept, Missing Constraint, Revised Concept, New Constraint and Modality Changes* is used. Finally, in the last step, the watermark techniques are used. The union reconciliation aims to merge requirements from multiple jurisdictions by analyzing the dissimilarities, identifying similar requirements between the two regulations, and merging the two near-equivalent requirements into one single requirement. In a minimum watermark, the requirements from one regulation that does not exist in the other regulation are omitted while in a disjoint watermark these requirements are preserved. These steps can be repeated for the third, fourth, ... and other regulations to capture all requirements in a single requirements set. This framework from Gordon et al. has been validated with a case study and patterns of dissimilarity have been explored.

Siena et al. [100] focus on extending the *Nòmos* Framework [105] to capture variability in laws. This work aims to capture the "antecedents" and "consequents" of clauses in the model of a law to analyze the "applicability" and "satisfiability" of these clauses to a set of requirements and evaluate their compliance. A norm is divided into five parts, which are "type", "holder", "beneficiary", "antecedent" and "consequent". A norm can be "satisfied" under a certain conditions and if it comes into effect, it becomes "applicable". To be

able to analyze the compliance, the approach includes situations, roles and six types of relations. With respect to the relations and the norm parts, the authors provide forward reasoning and backward reasoning for compliance analysis. The compliance evaluation gives either one of the following results: Compliance, Non-compliance, Tolerance, and Inconclusiveness.

The related work presented in this section aims to analyze legal requirements by separating them into several pieces such as roles, constraints, conditions, exceptions and clauses and try to resolve conflicts or handle multiple statements. In our work, however, we focus on the situations that can happen while dealing with more than one regulation, on how to model them with LEGAL-URN, and on how to ensure compliance and manage change.

7.2 Comparison between Multiple Regulations – Steps

In order to analyze the compliance of an organization to more than one regulation, we follow the methodology provided in Chapter 4 but with additional steps and with extensions to the Hohfeldian meta-model from Section 4.7.2.

Comparing multiple regulations implies comparing pairs of statements from different regulations to determine whether they are independent, similar, complementary, or contradictory. However, as each regulation can contain many statements, trying to analyze all possible pairs is not practical. This scalability issue can be mitigated by taking advantage of the structure of regulations. Indeed, related statements are often clustered under *sections* (and various levels of sub-sections). By matching pairs of related sections (from two regulations) first, we can focus on pairs of statements coming from each section, and prune out the pairs that involve statements of a matched section and statements of unmatched sections. Such section-focused pair-wise analysis can hence reduce the number of pairs to compare drastically.

We first extend the Hohfeldian meta-model of Chapter 4 to capture the <section>

concept. Figure 7.1 shows the extended meta-model, which now includes one new meta-class (Section, with a name attribute). Each Hohfeldian model is composed of 1 to many sections, and refers to possibly many statements. Each section can have 0 to many child sections (i.e., subsections) and each section or subsection can have 0 to many Hohfeldian statements. The rest of the Hohfeldian meta-model remains the same.

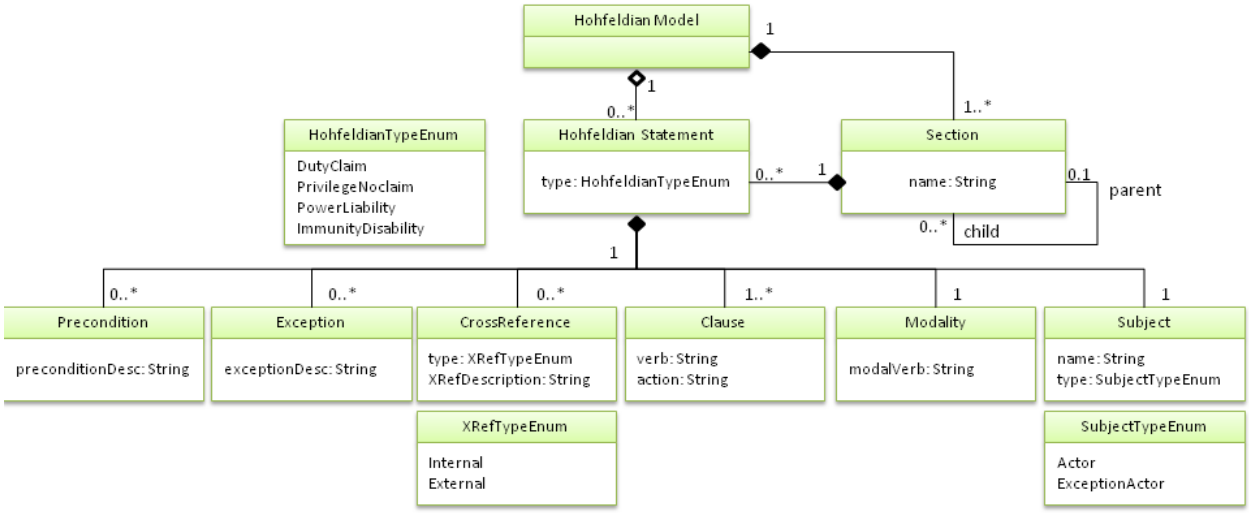

Figure 7.1: Extended Hohfeldian Meta-Model

The pair-wise comparison algorithm, shown in Figure 7.2, can then take advantage of this new data structure to classify matching pairs of regulation statements. Finding sections of a regulation that are relevant for the sections of another regulation requires manual effort from experts (e.g., lawyers). However, this can be done once for each pair of laws/regulations, so this effort can be amortize when this information is reused by multiple organizations. There are six cases considered in compareStatements(), and they are explained in Section 7.3.

Next, we modify the steps from Section 4.6 to include a step for pair-wise comparison and handling (Step 4'), which takes advantage of the new <section> concept.

- **Step 1.** Identify relevant legal and organizational documents.

```
Algorithm PairWiseComparison
Input hohfeldianModels: list of HohfeldianModel
Output pairedStatements: set of <Integer, HohfeldianStatement, HohfeldianStatement>

hm1, hm2: HohfeldianModel                          // two models to compare
sectionSet: set of Section                         // set of sections
sectionHM1, sectionHM2: Section                    // two sections to compare
statementHM1, statementHM2: HohfeldianStatement    // two statements to compare
index1, index2: Integer                            // two indices

// compare all unique pairs of models
pairedStatements = ∅
index1 = 0
while index1 < hohfeldianModels.size()
{
      hm1 = hohfeldianModels.at(index1)
      index2 = index1 + 1 // avoids comparing previously checked pairs
      while index2 < hohfeldianModels.size()
      {
            for each sectionHM1 in hm1
            {
                  // get, manually, the set of sections in hm2 that relate to sectionHM1
                  sectionSet = sectionHM1.manualSectionMatchingIn(hm2)
                  // compare the statements for pairs of relevant sections
                  for each sectionHM2 in sectionSet
                        for each statementHM1 in sectionHM1
                              for each statementHM2 in sectionHM2
                              {
                                    // determine case (1 to 6) and document it.
                                    case = compareStatements(statementHM1, statementHM2)
                                    pairedStatements.add(case, statementHM1, statementHM2)
                              }
            }
      }
}

return pairedStatements
```

Figure 7.2: PairWiseComparison Algorithm

- **Step 2.** Develop a Hohfeldian model for each of the regulations identified in Step 1: by classifying each statement of the legal document based on Hohfeld's classes of rights (defined in Section 2.2.2), while linking them to the source legal document (via source links).

- **Step 3.** Refine the *Power-Liability* and *Immunity-Disability* statements of the Hohfeldian model into multiple *Duty-Claim* or *Privilege-NoClaim* statements.

- **Step 4.** Develop the goal model of the law for each of the regulations and annotate the intentional elements with «Permission», «Obligation», «Precondition», «Exception», and «XRef» tags. Create source links to the legal documents, and compliance links to the Hohfeldian model.

- **NEW Step 4'.** Use the pair-wise comparison algorithm (Figure 7.2) to classify the various cases, and establish traceability links between the legal models for cases 2 to 5. The traceability links between low-level tasks of the two models are *weighted* traceability links with contribution factors at 100, while between matching pairs of high-level goals or actors from the two legal models we find *simple* traceability links (correlation links with contribution factors at 0). The *weighted* traceability links ensure that the satisfaction values of one legal model propagate to the other legal models connected to it. The *weighted* and *simple* traceability links follow the same concept as traceability links between two GRL models in Chapter 4.

- **Step 5.** Develop the business process model of law if necessary and link it to the goal model. Create source links to the legal documents, and responsibility links to the goal model. Note that we only compare Legal GRL models.

- **Step 6.** Develop the goal model and the business process model of the organizations. Create source links to the organization's procedure and policy documents, as well as responsibility links from the business process model to the goal model.

- **Step 7.** Identify the «Consequence» goals as the consequence of non-compliance.

- **Step 8.** Establish the links (compliance, traceability, and consequence) between the legal and organizational models.

At the very end of Chapter 4, we stated that the steps of the framework can be achieved by different roles, possibly played by different people inside or outside of the organization. For example, *expert legal modelers*, *business analysts* and *compliance officers* can be in charge of different parts of the framework. We also mentioned that an *expert legal modeler* (not necessarily part of any target organization) can create the Legal URN models for a law, a *business analyst* can be in charge of the organizational model, and an organization's *compliance officer* can add the links between organizational and legal models and analyze compliance. This separation of roles is especially important and useful for creating the legal models which can be used by several organizations. In addition, comparing multiple regulations and providing links between each pair of laws/regulations can be done once by a *expert legal modeler* and then shared with (or sold to) many organizations dealing with those sets of regulations. Such reuse helps amortize the manual effort invested in the manual modeling of regulations and their links.

In the above list of steps, steps 2, 3, 4, 4' and 5 can be done by a *expert legal modeler*, steps 1 (organizational documents) and 6 can be done by a *business analyst* and finally steps 1 (legal documents), 7 and 8, together with the compliance analysis and prioritization, can be done by the *compliance officer*.

7.3 Pair-wise Comparison of Two Statements

When dealing with more than one regulation (Step 4' in the previous section), the following cases involving two statements can be observed:

- Case 1 - There is nothing in common between the two statements.
- Case 2 - Both statements are similar to each other.
- Case 3 - One statement is complementary to the other statement.

- Case 4 - One statement is stricter than the other statement.
- Case 5 - One statement is a subset of the other statement.
- Case 6 - One statement contradicts the other statement.

The function compareStatement(Statement$_i$: HohfeldianStatement, Statement$_j$: HohfeldianStatement) from the algorithm shown in Figure 7.2, where Statement$_i$ comes from the first Hohfeldian model (hm1) and Statement$_j$ from the second model (hm2), is what is being defined in this section. Each of the six cases is discussed next. Note that <section>s of a statement are not compared as they have already been found to match by an *expert legal modeler*. In addition, cases 1, 2, and 6 are symmetric, but cases 3, 4, and 5 are asymmetric and hence need to be checked in both directions.

7.3.1 Case 1 - Nothing in Common between the Two Statements

Statement$_i$ is dealing with an issue different from Statement$_j$.

In this case, <clause> (<verb> and <action>), <precondition> and <exception> parts of each statement are different from each other. However, <actor> (i.e., a <subject> of type Actor), <modal verb> and <XRef> are not necessarily different. Two statements can be directed to the same subject, have the same type of modality and be related to the same cross-referenced statement but have different concerns.

Table 7.1 provides the summary of the comparison between two statements that have nothing in common.

In this case, to ensure the compliance with both of the regulations, it is necessary to model Statement$_j$ of hm2 as is, add it to the Legal GRL model, and provide the necessary links to the organizational GRL model (Step 5-8). There is no traceability link (simple or weighted) between the two Legal GRL models.

For example, Article 22(1) of PHIPA and Article 47(1) of the Health Care Consent Act (HCCA, 1996) [38] both deal with the concept of "incapacity".

Table 7.1: Case 1 - Nothing in Common between the Two Statements

Statement$_i$	**Statement**$_j$	**Comparison**
Section$_i$	Section$_j$	Matched by expert
Actor$_i$	Actor$_j$	-
Modal Verb$_i$	Modal Verb$_j$	-
Clause$_i$	Clause$_j$	Clause$_i$ $\cap$ Clause$_j$ = $\varnothing$
Precondition$_i$	Precondition$_j$	Precondition$_i$ $\cap$ Precondition$_j$ = $\varnothing$
Exception$_i$	Exception$_j$	Exception$_i$ $\cap$ Exception$_j$ = $\varnothing$
XRef$_i$	XRef$_j$	-

Article 22(1) of PHIPA states: ***Determination of incapacity*** - *An HIC that determines the incapacity of an individual to consent to the collection, use or disclosure of personal health information under this Act shall do so in accordance with the requirements and restrictions, if any, that are prescribed.*

Article 47(1) of HCCA states: ***Incapacity*** - *An evaluator shall, in the circumstances and manner specified in guidelines established by the governing body of the evaluator's profession, provide to persons found by the evaluator to be incapable with respect to admission to a care facility such information about the consequences of the findings as is specified in the guidelines.*

Article 22(1) of PHIPA discusses "incapacity of an individual to consent" and the responsibility of the HIC with respect to it while Article 47(1) of HCCA talks about "incapacity for treatment". As shown in Table 7.2, the <clause> and <precondition> of these two articles are dealing with two different issues. If a hospital needs to be compliant with both regulations, it is necessary to have both statements included in the Legal GRL model.

7.3.2 Case 2 - Both Statements are Similar to Each Other

Statement$_j$ of contains <actor> (<subject>), <modal verb>, <clause> (<verb> and <actions>), <precondition>, <exception> and <XRef> similar to those of Statement$_i$ (Table 7.3). For short, Statement$_i$ $\equiv$ Statement$_j$.

Table 7.2: Example for Case 1 (Nothing in Common)

Statement	**Statement**$_1$	**Statement**$_2$
Section	Determination of incapacity	Incapacity
Actor	An HIC	An evaluator
Modal Verb	Shall	Shall
Clause	Do so in accordance with the requirements and restrictions, [...]	Provide to persons found by the evaluator to be incapable with respect to admission to a care facility such information about [...]
Precondition	Determines the incapacity of an individual to consent to the collection, use or disclosure of PHI [...]	in the circumstances and manner specified in guidelines established by [...]
Exception	-	-
XRef	-	-

Table 7.3: Case 2 - Both Statements are Similar to Each Other

Statement$_i$	**Statement**$_j$	**Comparison**
Section$_i$	Section$_j$	Matched by expert
Actor$_i$	Actor$_j$	Actor$_i \equiv$ Actor$_j$
Modal Verb$_i$	Modal Verb$_j$	Modal Verb$_i \equiv$ Modal Verb$_j$
Clause$_i$	Clause$_j$	Clause$_i \equiv$ Clause$_j$
Precondition$_i$	Precondition$_j$	Precondition$_i \equiv$ Precondition$_j$
Exception$_i$	Exception$_j$	Exception$_i \equiv$ Exception$_j$
XRef$_i$	XRef$_j$	XRef$_i \equiv$ XRef$_j$

In this case, compliance with one statement ensures compliance with the other statement. However, to avoid any potential non-compliances in the face of change, it is necessary to model both of the statements in Legal GRL and use traceability links between the two Legal GRL model. The satisfaction values from one Legal GRL model is propagated to the other Legal GRL model via *simple* and *weighted* traceability links.

For instance, Article 25(2) **Transfer of request** in the Freedom of Information and Protection of Privacy Act (FIPPA, 2011) [79] states: *25 (2) Where an institution receives a request for access to a record and the head considers that another institution has a greater interest in the record, the head may transfer the request and, if necessary, the record to the other institution, within fifteen days after the request is received, in*

which case the head transferring the request shall give written notice of the transfer to the person who made the request. R.S.O. 1990, c. F.31, s. 25 (2).

Article 18(3) **Transfer of request** in Municipal Freedom of Information and Protection of Privacy Act (MFIPPA, 2007) [78] mentions: *18(3) If an institution receives a request for access to a record and the head considers that another institution has a greater interest in the record, the head may transfer the request and, if necessary, the record to the other institution, within fifteen days after the request is received, in which case the head transferring the request shall give written notice of the transfer to the person who made the request.*

Table 7.4 illustrates the comparison between the two articles:

Table 7.4: Example for Case 2 (Similar Statements)

Statement	**Statement**$_1$	**Statement**$_2$
Section	Transfer of request	Transfer of request
Actor	The head	The head
Modal Verb	May	May
Clause	Transfer the request [...] within fifteen days after the request is received	Transfer the request [...] within fifteen days after the request is received
Precondition	Where an institution receives a request for [...]	If an institution receives a request for [...]
Exception	-	-
XRef	-	-
Actor	The head [...]	The head [...]
Modal Verb	Shall	Shall
Clause	Give written notice [...]	Give written notice [...]

As illustrated, these two articles are addressing the same issue and have the same actors, preconditions, modal verbs, and clauses (without any exceptions or cross-references). Therefore, having a link between them (to manage change) and a link between one of them and the organization model will be enough for ensuring the compliance.

7.3.3 Case 3 - One Statement is Complementary to the Other Statement

Statement$_j$ and Statements$_i$ have their <actor> and <clause> in common or complementary. However, Statement$_j$ has more <precondition>(s), <exception>(s) or <XRef>(s) compared to Statement$_i$. <modal verb> for both statements are not necessarily similar but they are also NOT contradicting with each other. Table 7.5 formalizes this case.

Only one of <precondition>, <exception> or <XRef> needs to be a pure subset (the others can be equivalent). Note also that the same verification must be done by swapping Statement$_j$ and Statements$_i$.

Table 7.5: Case 3 - One Statement is Complementary to the Other Statement

Statement$_i$	**Statement$_j$**	**Comparison**
Section$_i$	Section$_j$	Matched by expert
Actor$_i$	Actor$_j$	Actor$_i \equiv$ Actor$_j \vee$ Actor$_i$ ***is-a*** Actor$_j$
Modal Verb$_i$	Modal Verb$_j$	-
Clause$_i$	Clause$_j$	Clause$_i \subseteq$ Clause$_j$
Precondition$_i$	Precondition$_j$	Precondition$_i \subset$ Precondition$_j$
Exception$_i$	Exception$_j$	Exception$_i \subset$ Exception$_j$
XRef$_i$	XRef$_j$	XRef$_i \subset$ XRef$_j$

In this case, we model both statements in Legal GRL models but only link one of the statements as well as the complementary part of the second statement to the organizational model (Step 5-8). Again, the part of the Legal GRL models that are similar are connected to each other by traceability links.

Article 44 from FIPPA states: ***Personal information banks*** - *A head shall cause to be included in a personal information bank all personal information under the control of the institution that is organized or intended to be retrieved by the individual's name or by an identifying number, symbol or other particular assigned to the individual.*

Article 10 of the Privacy Act [20] mentions: ***Personal information banks*** - *10.(1) The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that (a)*

has been used, is being used or is available for use for an administrative purpose; or (b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. This article also includes an exception rule: ***Exception for Library and Archives of Canada*** *- (2) Subsection (1) does not apply in respect of personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes.*

Table 7.6 presents the comparison between the two articles. Article 10(1-2) includes the same <actor> and <clause> as those in Article 44. However, Article 10(1-2) contains additional <precondition> and <exception> that Article 44 does not entail.

Table 7.6: Example for Case 3 (Complementary Statements)

Statement	**Statement**$_1$	**Statement**$_2$
Section	Personal information banks	Personal information banks
Actor	A head	The head of a government institution
Modal Verb	Shall	Shall
Clause	Cause to be included in a personal information bank all personal information under the control of the institution	Cause to be included in personal information banks all personal information under the control of the government institution
Precondition 1	Is organized or intended to be retrieved by the individual's name or by an identifying number, [...]	Is organized or intended to be retrieved by the name of an individual or by an identifying number, [...]
Precondition 2	-	Has been used, is being used or is available for use for an administrative purpose
Exception	-	Subsection (1) does not apply in respect of personal information under the custody or control of the Library and Archives of Canada [...]
XRef	-	-

7.3.4 Case 4 - One Statement is Stricter than the Other Statement

Statement$_j$ provides stricter modality or clause than Statements$_i$. In this case, <modal verb> in Statement$_j$ indicates an obligation while in Statements$_i$ it indicates a permission, or the <clause> in Statement$_j$ is stricter (e.g., in terms of time) than the <clause> in Statement$_i$. The other parts in both statements remain similar (see Table 7.7). Note again that the same verification must be done by swapping Statement$_j$ and Statements$_i$.

Note that only one of the conditions for <modal verb> or <clauses> needs to be satisfied.

Table 7.7: Case 4 - One Statement is Stricter than the Other Statement

Statement$_i$	**Statement$_j$**	**Comparison**
Section$_i$	Section$_j$	Matched by expert
Actor$_i$	Actor$_j$	Actor$_i \equiv$ Actor$_j$
Modal Verb$_i$	Modal Verb$_j$	Modal Verb$_j$ ***is-stricter-than*** Modal Verb$_i$
Clause$_i$	Clause$_j$	Clause$_j \implies$ Clause$_i$
Precondition$_i$	Precondition$_j$	Precondition$_i \equiv$ Precondition$_j$
Exception$_i$	Exception$_j$	Exception$_i \equiv$ Exception$_j$
XRef$_i$	XRef$_j$	XRef$_i \equiv$ XRef$_j$

In this case, it is only necessary to be compliant with the stricter statement, i.e., being compliant with Statement$_j$ implies compliance with Statement$_i$. However, it is also up to the organization to decide to be compliant with which regulation. If an organization decides to be compliant with the less strict statement, it will have the non-compliance consequences which are handled in the Legal-URN framework in Chapter 4.

Similar to case 2 in 7.3.2, to be able to manage changes, we model both of the statements in Legal GRL and link the intentional elements and actors of both models to each other via traceability links.

Article 47(2) - Right of Correction of FIPPA states: *Every individual who is given access under subsection (1) to personal information is entitled to,(c) require that any person or body to whom the personal information has been disclosed* ***within the year***

before the time a correction is requested *or a statement of disagreement is required be notified of the correction or statement of disagreement. R.S.O. 1990, c. F.31, s. 47 (2).*

Article 12(2) of the Privacy Act [20] mentions: *Every individual who is given access under paragraph (1)(a) to personal information that has been used, is being used or is available for use for an administrative purpose is entitled to (c) require that any person or body to whom that information has been disclosed for use for an administrative purpose* ***within two years prior to the time a correction is requested*** *or a notation is required under this subsection in respect of that information (i) be notified of the correction or notation, and [...]*

Table 7.8: Example for Case 4 (Stricter Statement)

Statement	**Statement**$_1$	**Statement**$_2$
Section	Right of Correction	Right of Correction
Actor	Every individual	Every individual
Modal Verb	Is entitled to	Is entitled to
Clause	Requires that any person or body [...] **within the year before the time a correction is requested** or [...]	Requires that any person or body [...] **within two years prior to the time a correction is requested** or [...]
XRef	-	-
Exception	-	-
Precondition	Who is given access under subsection (1) to personal information	Who is given access under paragraph (1)(a) to personal information that has been used, [...]

As illustrated, these two articles are talking about the right of correction under the same condition. However, Article 12(2) gives more time for correction than Article 47(2) (hence, the latter is stricter than the former).

7.3.5 Case 5 - One Statement is a Subset of the Other Statement

Statement$_j$ includes <actor> and <exception> similar to those of Statement$_i$, with some additional <clause> and potentially additional <precondition> and <XRef>. This

means Statement$_j$ includes further rules. For example, Statement$_i$ could deal with the disclosure of PHI to hospital researchers whereas Statement$_j$ would deal with disclosure of PHI to hospital researchers as well as external researchers. The formalization in Table 7.9 is again asymmetric, therefore the same verification must be done by swapping Statement$_j$ and Statements$_i$. <modal verb> for both statements are not necessarily similar but they are also *not* contradicting each other.

Table 7.9: Case 5 - One Statement is a Subset of the Other Statement

Statement$_i$	**Statement$_j$**	**Comparison**
Section$_i$	Section$_j$	Matched by expert
Actor$_i$	Actor$_j$	Actor$_i$ $\equiv$ Actor$_j$ $\vee$ Actor$_i$ ***is-a*** Actor$_j$
Modal Verb$_i$	Modal Verb$_j$	-
Clause$_i$	Clause$_j$	Clause$_i$ $\subset$ Clause$_j$
Precondition$_i$	Precondition$_j$	Precondition$_i$ $\subset$ Precondition$_j$
Exception$_i$	Exception$_j$	Exception$_i$ $\equiv$ Exception$_j$
XRef$_i$	XRef$_j$	XRef$_i$ $\subset$ XRef$_j$

Similar to the previous case, compliance with the superset statement is enough, though both statements need to be modeled and linked through traceability links.

Article 53 (1-2) in PHIPA states: ***Request for access*** - *(1) An individual may exercise a right of access to a record of PHI by making a written request for access to the HIC that has custody or control of the information.* ***Detail in request*** - *(2) The request must contain sufficient detail to enable the health information custodian to identify and locate the record with reasonable efforts. .*

Article 24 (1) of FIPPA mentions: ***Request*** - *A person seeking access to a record shall, (a) make a request in writing to the institution that the person believes has custody or control of the record; (b) provide sufficient detail to enable an experienced employee of the institution, upon a reasonable effort, to identify the record; and (c) at the time of making the request, pay the fee prescribed by the regulations for that purpose.*

The actor in Article 53 (1-2), an individual, is equivalent to the actor "person" in Article 24(1). Both articles are dealing with requests for access and their first two clauses

are in common. Article 24 (1) includes an additional clause and one more precondition than Article 53 (1-2) (see comparison in Table 7.10).

Table 7.10: Example for Case 5 (Subset of Other Statement)

Statement	**Statement**$_1$	**Statement**$_2$
Section	Request for access, Detail in request	Request
Actor	An individual	A person
Modal Verb	May	Shall
Clause 1	Exercise a right of access to a record of PHI by making a written request for access to the HIC that has custody or control of the information	Make a request in writing to the institution that the person believes has custody or control of the record
Clause 2	Contain sufficient detail to enable the health information custodian to identify and locate the record with reasonable efforts	Provide sufficient detail to enable an experienced employee of the institution, upon a reasonable effort, to identify the record
Clause 3	-	Pay the fee prescribed by the regulations for that purpose
Precondition	-	Seeking access to a record
Exception	-	-
XRef	-	-

7.3.6 Case 6 - One Statement Contradicts the Other Statement

Statement$_j$ is in conflict with Statement$_i$ when both statements have a common <actor>, but at least one of the pairs of <modal verb>, <clause>, <precondition>, <exception> or <XRef> is contradictory (expressed here with the $\lightning$ symbol).

In this case, complying with the first statement results in non-compliance with the second statement, and vice versa. To resolve the conflict however, it is necessary to ask a subject matter expert (e.g., a lawyer, a legal consultant, or a policy analyst), and incorporate the solution into the Legal GRL model.

Article 12(1) of the Privacy Act states: ***Right of access*** - *Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of*

Table 7.11: Case 6 - One Statement Contradicts the Other Statement

Statement$_i$	**Statement**$_j$	**Comparison**
Section$_i$	Section$_j$	Matched by expert
Actor$_i$	Actor$_j$	Actor$_i \equiv$ Actor$_j$
Modal Verb$_i$	Modal Verb$_j$	Modal Verb$_i$ $\lightning$ Modal Verb$_j$
Clause$_i$	Clause$_j$	Clause$_i$ $\lightning$ Clause$_j$
Precondition$_i$	Precondition$_j$	Precondition$_i$ $\lightning$ Precondition$_j$
Exception$_i$	Exception$_j$	Exception$_i$ $\lightning$ Exception$_j$
XRef$_i$	XRef$_j$	XRef$_i$ $\lightning$ XRef$_j$

subsection 2(1) of the Immigration and Refugee Protection Act has a right to and shall, on request, be given access to (a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.

Article 9(1) of the Personal Information Protection and Electronic Documents Act (PIPEDA) [37] states: ***When access prohibited*** *- 9. (1) Despite clause 4.9 of Schedule 1, an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party.*

As shown in Table 7.12, Article 12(1) obliges organizations to give access to an individual (even if it has a precondition about the revealing of personal information about a third party) while Article 9(1) obliges organizations *not* to give access to an individual. These two articles are in contradiction with each other. To be able to resolve this conflict, it is necessary to get advice from a legal expert in order to decide whether the access to the personal information reveals the conflict or not. Based on the result of the consultation, it is possible to decide which one of these two Articles applies to the organization.

Table 7.12: Example for Case 6 (Contradicts the Other Statement)

Statement	**Statement**$_1$	**Statement**$_2$
Section	Right of access	When access prohibited
Actor	An individual	An organization
Modal Verb	Shall	Shall not
Clause 1	Be given access to (a) any personal information about the individual [...]	Give an individual access to personal information
Precondition	-	If doing so would likely reveal personal information about a third party.
Exception	-	-
XRef	-	-

7.4 Summary of Pair-Wise Comparison

Table 7.13 summarizes the result of the analysis of pair-wise comparison cases. Sections from each statement were previously matched by experts (and hence are not included in this table). Note that for most cases, the conditions on the various parts of a statement are composed through a logical AND. However, for case 6, the five conflict conditions are composed through a logical OR.

Table 7.13: Summary Table - Pair-Wise Comparison

Statement	**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**
Actor	-	$\text{Actor}_i \equiv \text{Actor}_j$	$\text{Actor}_i \equiv \text{Actor}_j \vee \text{Actor}_i$ ***is-a*** Actor_j	$\text{Actor}_i \equiv \text{Actor}_j$	$\text{Actor}_i \equiv \text{Actor}_j \vee \text{Actor}_i$ ***is-a*** Actor_j	$\text{Actor}_i \equiv \text{Actor}_j$
Modal Verb	-	$\text{Modal Verb}_i \equiv \text{Modal Verb}_j$	-	Modal Verb_j ***is-stricter-than*** Modal Verb_i	-	$\text{Modal Verb}_i \lightning \text{Modal Verb}_j$
Clause	$\text{Clause}_i \cap \text{Clause}_j = \varnothing$	$\text{Clause}_i \equiv \text{Clause}_j$	$\text{Clause}_i \subseteq \text{Clause}_j$	$\text{Clause}_j \implies \text{Clause}_i$	$\text{Clause}_i \subset \text{Clause}_j$	$\text{Clause}_i \lightning \text{Clause}_j$
Precondition	$\text{Precondition}_i \cap \text{Precondition}_j = \varnothing$	$\text{Precondition}_i \equiv \text{Precondition}_j$	$\text{Precondition}_i \subset \text{Precondition}_j$	$\text{Precondition}_i \equiv \text{Precondition}_j$	$\text{Precondition}_i \subset \text{Precondition}_j$	$\text{Precondition}_i \lightning \text{Precondition}_j$
Exception	$\text{Exception}_i \cap \text{Exception}_j = \varnothing$	$\text{Exception}_i \equiv \text{Exception}_j$	$\text{Exception}_i \subset \text{Exception}_j$	$\text{Exception}_i \equiv \text{Exception}_j$	$\text{Exception}_i \equiv \text{Exception}_j$	$\text{Exception}_i \lightning \text{Exception}_j$
XRef	-	$\text{Xref}_i \equiv \text{Xref}_j$	$\text{XRef}_i \subset \text{XRef}_j$	$\text{XRef}_i \equiv \text{XRef}_j$	$\text{XRef}_i \subset \text{XRef}_j$	$\text{XRef}_i \lightning \text{XRef}_j$

7.5 Summary

In this chapter, we first reviewed related work on how to handle multiple regulations and then discussed the steps needed to perform comparisons between regulations. Next, we discussed the extension to the Hohfeldian meta-model to support sections as well as an algorithm that determines the different cases that can happen when comparing two statements from two different regulations. Sections are used in this algorithm to reduce the number of pairs of statements to compare. Finally, we explained these cases in detail based on the meta-model and provided some handling mechanisms for each case, with examples. We also discussed how the result of the comparison can be modeled and linked in Legal GRL models. If two statements have parts in common, it is not necessary to link both of them to the organization. To ensure compliance to both regulations, the common parts of the regulations are linked to each other via *simple* or *weighted* traceability links. The satisfaction values can propagate from one model to the to other via *weighted* traceability links with a 100 contribution value.

The next chapter will illustrate the application of such improved approach on an extension of our healthcare case study where the organization this time must comply with multiple regulations.

Chapter 8

Case Study 2: Multiple Regulations and The Ontario Hospital

This chapter aims to evaluate our Legal-URN framework via a second case study. We added three more regulations to the case study described in Chapter 6. We follow the steps mentioned in Chapter 7 to handle multiple regulations and add the new statements to the Legal-URN models made in Chapter 6. We then analyze the compliance based on the new regulatory requirements and prioritize the non-compliant instances. Finally, we provide the lesson learned from this case study.

8.1 Case Study Overview

The second case study extends the first one described in Chapter 6 by adding three new regulations: Freedom of Information and Protection of Privacy Act (FIPPA) [79], Quality of Care Information Protection Act, 2004 (QoCIPA) [39] and Health Care Consent Act, 1996 (HCCA) [38]. However, all of the models created in the first case study are still valid.

In this case study, The Ontario Hospital aims to improve its quality of care. To that aim, the hospital discloses current quality of care information to their management

and healthcare providers. The hospital also hires a team of external researchers to analyze the quality of care based on the information collected. To increase their revenues and minimize their costs, the hospital collects and uses Personal Information (PI) and Personal Health Information (PHI), and discloses that information for fundraising to external agencies/researchers. In addition, the hospital needs to ensure that patients provide their consent for treatment. As a result of all these activities, the hospital has to ensure that it is compliant with the relevant parts of several regulations.

8.2 Step 1 – Identify Relevant Legal and Organizational Documents

Based on the case study overview in the previous section, the hospital needs to comply with some parts of the following three regulations, in addition to PHIPA: a) Quality of Care Information Protection Act, 2004 (QoCIPA), b) Freedom of Information and Protection of Privacy Act (FIPPA), and c) Health Care Consent Act, 1996 (HCCA).

In QoCIPA, the hospital must ensure its compliance to the statements 3, 4(1) and 4(3)-(6), which are dealing with the collection, use and disclosure of information. In FIPPA, statements 38(2), 39(1)(2), 41(1d)(2), 42(1o,1i), 42(2) and 42(3), which are related to the collection, use and disclosure of PI, have been identified. Finally, in HCCA, the hospital has to comply with statements 10(1), 11(1) and 11(4). These statements explain the requirements for consent for treatment, elements of consent, types of consents, and withdrawal conditions.

8.3 Steps 2 and 3 – Developing and Refining a Hohfeldian Model of Law

In Section 8.2, we identified ten articles from three regulations with which the hospital has to comply, in addition to those from PHIPA. In the next step, we build the Hohfeldian model of each regulation and identify Duty-Claim, Privilege-NoClaim, Power-Liability, and Immunity-Disability statements.

These articles have multiple statements. There are 16 identifiable statements in total, including 11 Duty-Claim and 5 Privilege-NoClaim.

For example, statement 4(1)-Quality of care information of the Quality of Care Information Protection Act (QoCIPA) states that *Despite PHIPA, no person **shall** disclose quality of care information **except** as permitted by this Act.*

With respect to the rules identified in Chapter 4 and the Hohfeldian meta-model in Figure 7.1, we analyze this statement.

This statement, which contains the modal verb **shall**, is of type Duty-Claim. However, it also includes an exception where a person **may** disclose quality of care information to another person, only if it is permitted by this act (i.e., internally cross-referenced to other statements in this act).

Table 8.1 illustrates the various parts of Article 4(1):

Table 8.1: Quality of Care Information Protection Act - Statement 4(1)

Section	Quality of care information
Actor	A Person
Modal Verb	Shall
Clause	Not disclose quality of care information
Exception	Permitted by this act
XRef	Despite PHIPA

The other statements and their Hohfeldian models are explained in Appendix E.

8.4 Steps 4 and 5 – Developing Legal GRL and Legal UCM

After having defined the Hohfeldian models of the regulations, we transform them to Legal GRL and/or Legal UCM models. Before modeling the new statements, first, we model the high-level goals of all of the acts in one diagram. Each of these high-level goals (shown as softgoals) are related to one or many statements in the regulations we analyzed in Chapter 6 as well as this chapter, and they will expand to separate Legal GRL models based on each article. Figure 8.1 illustrates this high-level GRL diagram.

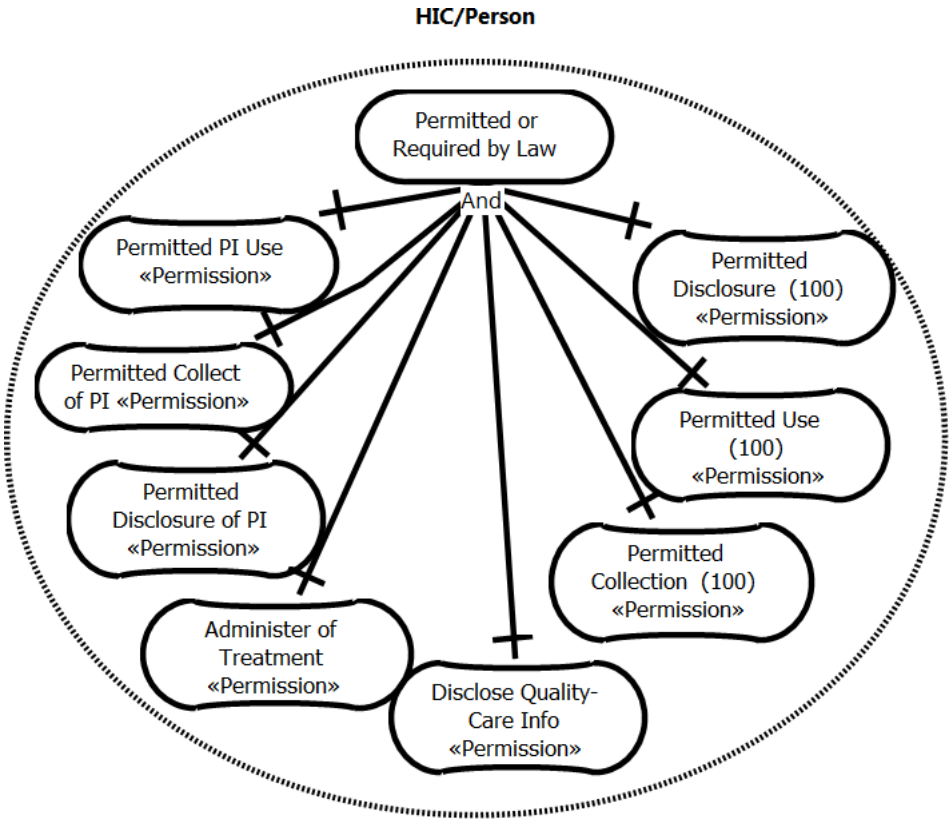

Figure 8.1: High-Level Softgoals of Legal GRL Model

Similar to the first case study explained in Chapter 6, we follow the steps from Section 4.7.3 for Legal GRL models. We transform the Duty-Claim and Privilege-NoClaim statements to «Obligation» and «Permission» goals, respectively. Next, we model the

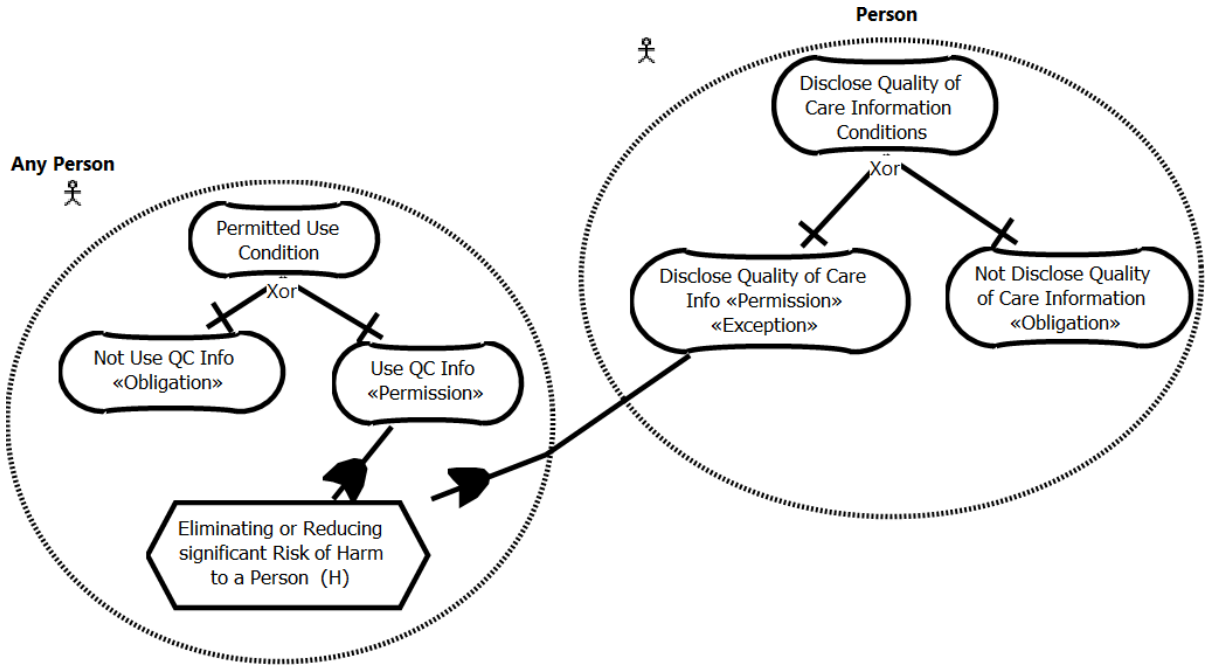

Figure 8.2: Quality of Care Information - Statement 4(1)(4)(5)

<actor>, <precondition>, <exception>, and <XRef> with actor, precondition, exception, and cross-reference elements in Legal GRL, and include the links between them.

For example, the Legal GRL model for the statement 4(1) we analyzed in Section 8.3 is shown on the right-hand side of Figure 8.2. The actor, a person is modeled as a GRL actor. The clause Not disclose quality of care information is modeled as an «Obligation» goal whereas the exception clause Permitted by this act is modeled as the goal Disclose Quality of Care Information, which combines «Permission» and «Exception» stereotypes. The left-hand side of this Legal GRL model is related to statement 4(4), which is covered in Appendix E, together with the rest of the Legal GRL models.

Note that in this case study, Step 5 can be done before or after Step 4' without any impact. Furthermore, since this case study expands the case study in Chapter 6, the Legal UCM models of the previous case still apply to this one. However, we do not include them here since they were presented before.

8.5 Step 4' – Analyzing New Regulations through Comparisons

Once the Legal GRL models of the new regulations' statements are built, we perform pair-wise comparisons between each two relevant statements, as explained in Section 7.3. We start the comparison between the PHIPA articles of Chapter 6 and the new articles mentioned in this chapter.

In Chapter 6, we mentioned that the hospital needs to comply with Articles 10 (Information practices), 11 (Accuracy), 12 (Security), 18 (Elements of consent), 29 (Requirement for consent), 31 (Use and disclosure of personal health information), parts of 36 (Indirect collection), parts of 37 (Permitted Use), 38 (Disclosures related to providing health care), and parts of 44 (Disclosure for research) from PHIPA. The only statements relevant to the hospital are 1a-d in Article 36; 1a,1d, 1i and 3 in Article 37; 1 in Article 38; and 1-6 in Article 44. In addition, since now the hospital discloses PHI for fundraising, they have to comply with Article 32a as well. Therefore, we need to make the pair-wise comparison between the statements in these articles and the statements mentioned in this chapter.

We first start by comparing PHIPA with the Quality of Care Information Protection Act (QoCIPA), then with the Freedom of Information and Protection of Privacy Act (FIPPA) and finally with the Health Care Consent Act (HCCA). Note that comparisons between QoCIPA and FIPPA, between QoCIPA and HCCA, and between FIPPA and HCCA would also be desirable in practice, but they are not required for the purpose of this case study.

In the first step for each of these regulations, we identify the sections that are omitted from the pair-wise comparison and then compare the remaining articles two by two.

In QoCIPA, we compare Article 3 (Disclosure to quality of care committee) and 4 (Quality of care information) to the articles in PHIPA. By comparing the sections, we identified that Articles 3 and 4 do not have anything in common with Articles 10, 11,

12, 18, 32, 36, and 37. Thus, we only need to compare Articles 3 and 4 in QoCIPA with Articles 29, 31, 38(1) and 44(1)-(6) in PHIPA.

Article 3 states: *Despite this Act and PHIPA, a person **may** disclose any information to a quality of care committee for the purposes of the committee.* Tables 8.2 summarizes the statement's parts.

Table 8.2: Quality of Care Information Protection Act - Article 3

Section	Disclosure to quality of care committee
Actor	A person
Modal Verb	May
Clause	Disclose any information to a quality of care committee for the purposes of the committee.
XRef	Despite PHIPA

When comparing this Article 3 with Articles 29 and 31 of PHIPA (Table 8.3 and Table 8.4), we identify a conflict between the clauses. However, the law itself provides a resolution for this conflict. Article 3 cross-references PHIPA by mentioning "Despite PHIPA". This means that in the case of a conflict, this article gets priority over PHIPA. In addition, Articles 29 and 31 provide an exception that states that if any of the pre-conditions are satisfied, then the disclosure is permitted.

Therefore, in our case study, when disclosing quality of information to the quality of care committee, this article gives priority to QoCIPA and we only need to link the Legal GRL model of Article 3 to the organizational model for quality of care.

Table 8.3: Pair-Wise Comparison of Article 3 of QoCIPA and Article 29 of PHIPA

Statement	**Statement**$_1$	**Statement**$_2$
Section x	Disclosure to quality of care committee	Requirement for consent
Actor	A person	An HIC
Modal Verb	May	Shall
Clause	Disclose Any information to a quality of care committee for the purposes of the committee.	[Not] collect, use or disclose PHI about an individual
Exception	-	May collect, use or disclose PHI
Precondition 1	-	It has the individual's consent, and the collection, use or disclosure [...] is necessary (or)
Precondition 2	-	The collection, use or disclosure is [...] permitted
XRef	Despite PHIPA	-

Table 8.4: Pair-Wise Comparison of Article 3 of QoCIPA and Article 31 of PHIPA

Statement	**Statement**$_1$	**Statement**$_2$
Section x	Disclosure to quality of care committee	Use and disclosure of personal health information
Actor	A person	An HIC
Precondition	-	that collects PHI in contravention of this Act
Modal Verb	May	Shall
Clause	Disclose Any information to a quality of care committee for the purposes of the committee.	[Not] use it or disclose it
Exception	-	Unless = May collect, use or disclose PHI
Precondition 1	-	Required by law to do so
XRef	Despite PHIPA	-

Both Article 3 of QoCIPA and Article 44(1) of PHIPA are giving permission to disclose any information or PHI to a group: Article 3 gives permission to disclose to a quality of care committee while Article 44(1) permits disclosure to a researcher. As shown in Table 8.5, these two articles are complementary (case 3), with one that has more conditions than the other.

With GRL, we model both articles and provide traceability links between the additional part of Article 3 and the organizational model for the case of disclosing to the researcher.

Table 8.5: Pair-Wise Comparison of Article 3 of QoCIPA and Article 44(1) of PHIPA

Statement	**Statement**$_1$	**Statement**$_2$
Section	Disclosure to quality of care committee	Disclosure for research
Actor	A person	An HIC
Modal Verb	May	May
Clause	Disclose any information to [a quality of care committee for the purposes of the committee.]	Disclose PHI about an individual to [a researcher if the researcher]
Precondition 1	-	Submits to the custodian [...]
Precondition 2	-	Enters into the agreement required by subsection
Exception	-	Unless = May collect, use or disclose PHI
XRef	Despite PHIPA	-

Table 8.6 presents the pair-wise comparison between Article 3 of QoCIPA and 44(3) of PHIPA.

The rest of the pair-wise comparison are presented in Appendix E.

Tables 8.7, 8.8 and 8.9 summarize the pair-wise comparisons between QoCIPA and PHIPA, FIPPA and PHIPA as well as HCCA and PHIPA, respectively.

Table 8.6: Pair-Wise Comparison of Article 3 of QoCIPA and Article 44(3) of PHIPA

Statement	**Statement**$_1$	**Statement**$_2$
Section	Disclosure to quality of care committee	Disclosure for research
Actor	A person	A Research Ethic Board
Modal Verb	May	Shall
Clause	Disclose Any information to a quality of care committee for the purposes of the committee.	Consider the matters that it considers relevant, including (a) to (d)
Precondition	-	When deciding whether to approve a research plan that a researcher submits to it
Exception	-	-
XRef	Despite PHIPA	-

Table 8.7: Summary of Pair-Wise Comparisons between QoCIPA and PHIPA

Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**
17	1	3	-	2	3

The comparisons between QoCIPA and PHIPA show the presence of case 2 (4(5) vs 31), case 3 (3,4 vs 44(1); 4(5) vs 29), case 5 (3, 4 (1)(3)(4)(6) vs 38(1)) and case 6 (3 vs 29, 31; 4(5) vs 37(1)).

Table 8.8: Summary of Pair-Wise Comparisons between FIPPA and PHIPA

Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**
37	-	4	-	3	-

The comparisons between FIPPA and PHIPA show the presence of case 3 (38(2) vs 29; 41 vs 37; 41, 42 vs 32) and case 5(38(2) vs 36; 41 vs 29,31).

Table 8.9: Summary of Pair-Wise Comparisons between HCCA and PHIPA

Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**
21	1	-	-	-	-

Finally, the comparisons between HCCA and PHIPA show the presence of case 2 between Article 11 and Article 18.

As stated earlier, for cases 2 to 5 of these comparisons, we link the Legal GRL models together via traceability links. Figure 8.3 shows the connection between Article 18 of PHIPA (left-hand side) and Article 11 of HCCA (right-hand side). Also shown at the bottom are the tasks connected to each other with traceability links with contribution

values of 100. Therefore, satisfying HCCA is enough. In addition, the high-level goal Consent Implied or Expressed is connected through *simple* traceability links (shown as correlation without contribution values) to PHIPA goals Have Implied Consent and Have Expressed Consent. The two actors are also connected to each other with a URN link, for traceability.

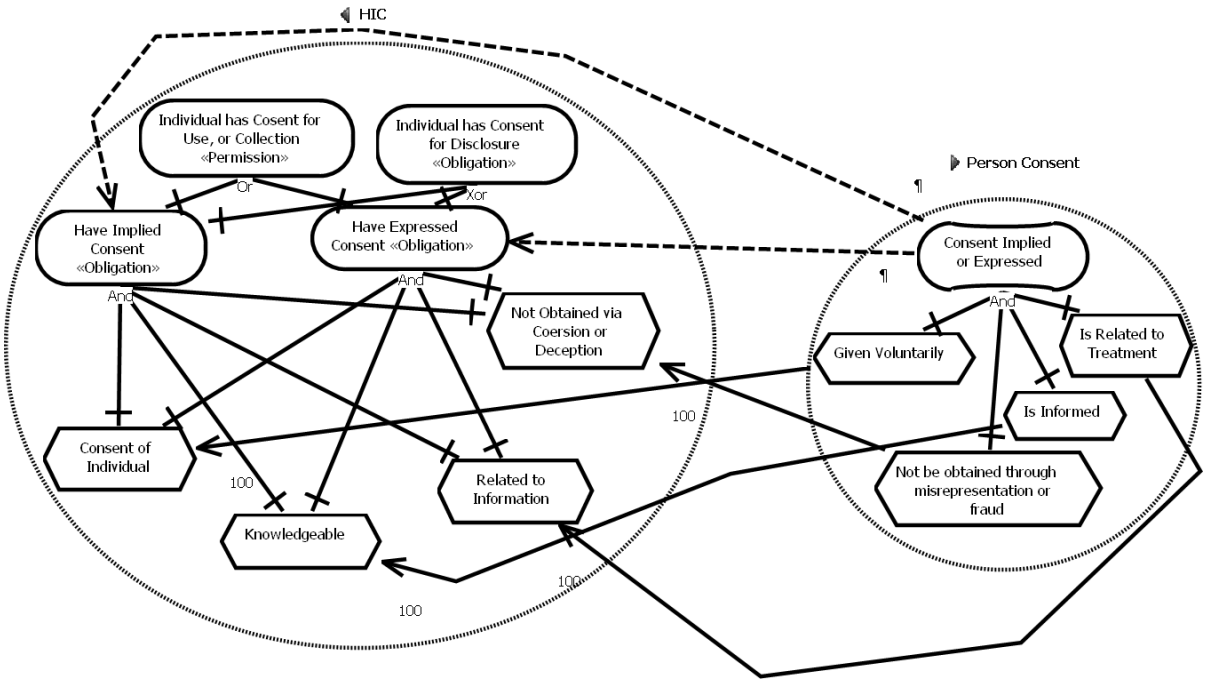

Figure 8.3: Example of Links between Article 18 of PHIPA (Left) and Article 11 of HCCA (Right)

In this case study, we acted as the *expert legal modeler* and have done the steps 2, 3, 4, 4' and 5 ourselves. However, these steps can be done by an expert legal modeler external to the organization.

8.6 Step 6 – Developing Organizational GRL and UCM

In Chapter 6, we identified and ranked five high-level goals (modeled as softgoals) for the hospital. These goals were: Provide Better Healthcare (PBH); Improve Quality of Services

(IQS); Protect Privacy and Confidentiality of PHI (PPC); Increase Understanding of Public Health (IUPH); and Minimizing Cost (MC).

In addition to the five softgoals, five PHIPA-related goals contributing to the five above softgoals were also defined: Disclose PHI to Researcher; Disclose PHI to Hospital Employees; Collect, Use or Disclose PHI to Obtain Payment; Collect, Use or Disclose PHI to Monitor, Verify or Reimburse Claim; and Collect, Use or Disclose PHI to Investigate Breach.

In this chapter, we described additional activities the hospital deals with. Based on these two activities, two more regulation-related goals are identified: Disclose Quality of Care Information and Disclose PI for Fundraising. These two goals also contribute to the above softgoals. We model these two goals in two separate but related GRL diagrams, and we add the contributions from these two goals to the five hospital softgoals. Figure 8.4 and Table 8.10 show the contributions and their values. We also modify the contribution values from Table 6.3 to include the two new goals' contributions.

Table 8.10: Hospital Goals to Softgoals Contribution Values

	PBH	**IQS**	**PPC**	**IUPH**	**MC**
... PHI to Researcher	20	10	-20	25	10
... PHI to Hospital Employees	50	50	-20	50	-
... PHI to Obtain Payment	-	-	-20	-	25
... PHI to Monitor, ... Claim	-	-	-20	-	25
... PHI to Investigate Breach	-	20	100	-	20
... Quality of Care Information	20	20	-20	25	-
... PI for Fundraising	10	-	-20	-	20

The hospital (Actor Hospital) discloses the quality of care information to the doctors (Actor Doctor) of their hospital (healthcare providers) to use the quality of care information (Goal Use Quality of Care Information) for analyzing the quality of care (Task Analyze Quality of Care in the hospital as well as eliminating the risk of harm (Task Eliminate Risk of Harm to an Individual) to the patients of the hospital. In addition, the hospital disclose these informations to the external researcher (Actor External Researcher) to perform some analysis. This model is shown in Figure 8.5. Note that the rest of the elements of the diagram are similar to the first case study.

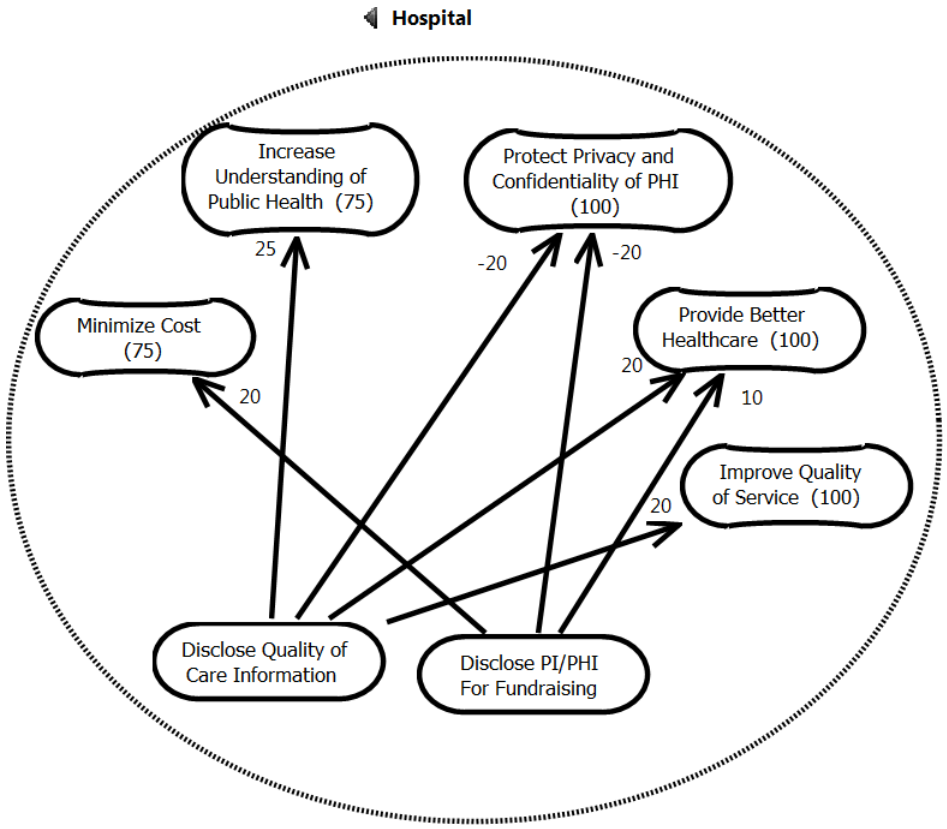

Figure 8.4: Hospital High-Level GRL Model - 2

The hospital (Actor Hospital) discloses the PI for fundraising to the external researcher (Actor External Researcher) to perform some research (Goal Perform Research on New Diseases). The hospital provides notice to the individual about the fundraising at the time of the disclosure (Task Give Notice to Individual at The Time of Disclosure) and sign an agreement (Task Sign an Agreement) to ensure the hospital meets the requirements for notices (Task To Ensure Meeting Notice Requirements) and it discloses the PI disclosed to the patient when requested (Task To Ensure Disclosure of Disclosed PI upon Individual Request). The model is illustrated in Figure 8.6.

Finally, the hospital that Disclose PHI to Hospital Employees for treatment (Goal Cure Patient) has to make sure to obtain an informed, voluntarily and relevant consent from the patient. We modified the previous GRL model for Disclose PHI to Hospital Employees to address this. Figure 8.7 presents the GRL model with its modification.

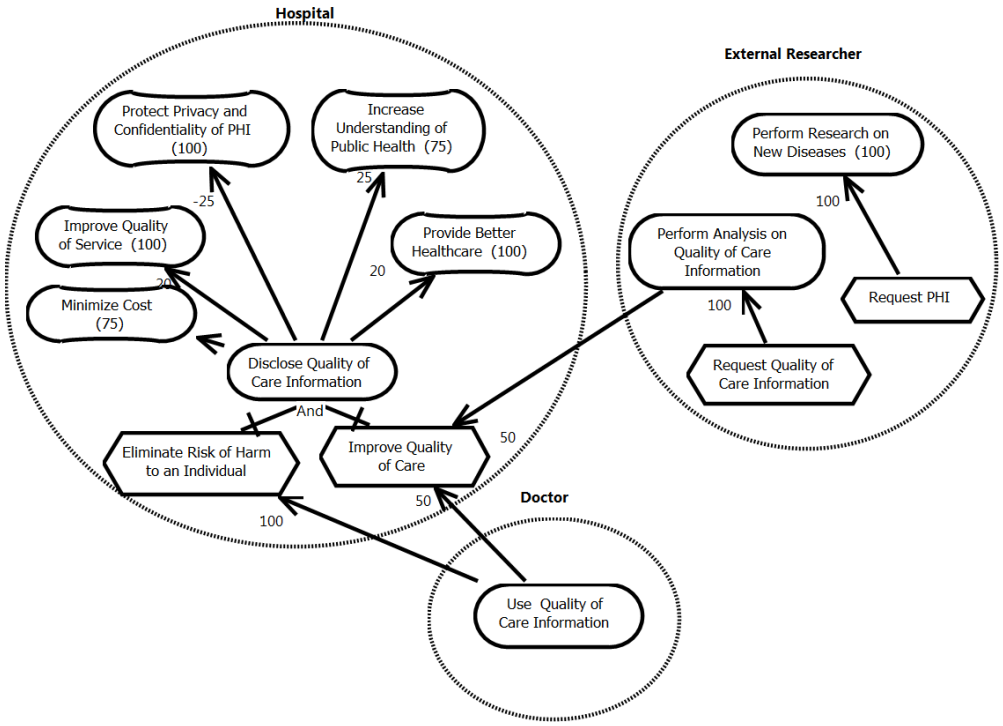

Figure 8.5: Hospital Model - Disclose Quality of Care Information

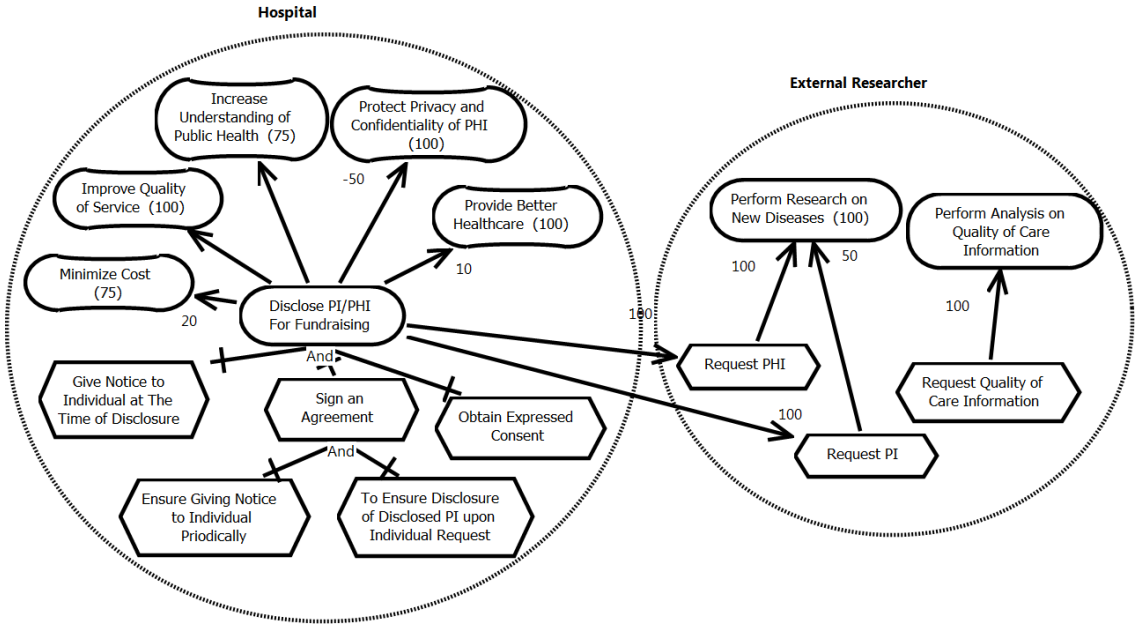

Figure 8.6: Hospital Model - Disclose PI for Fundraising

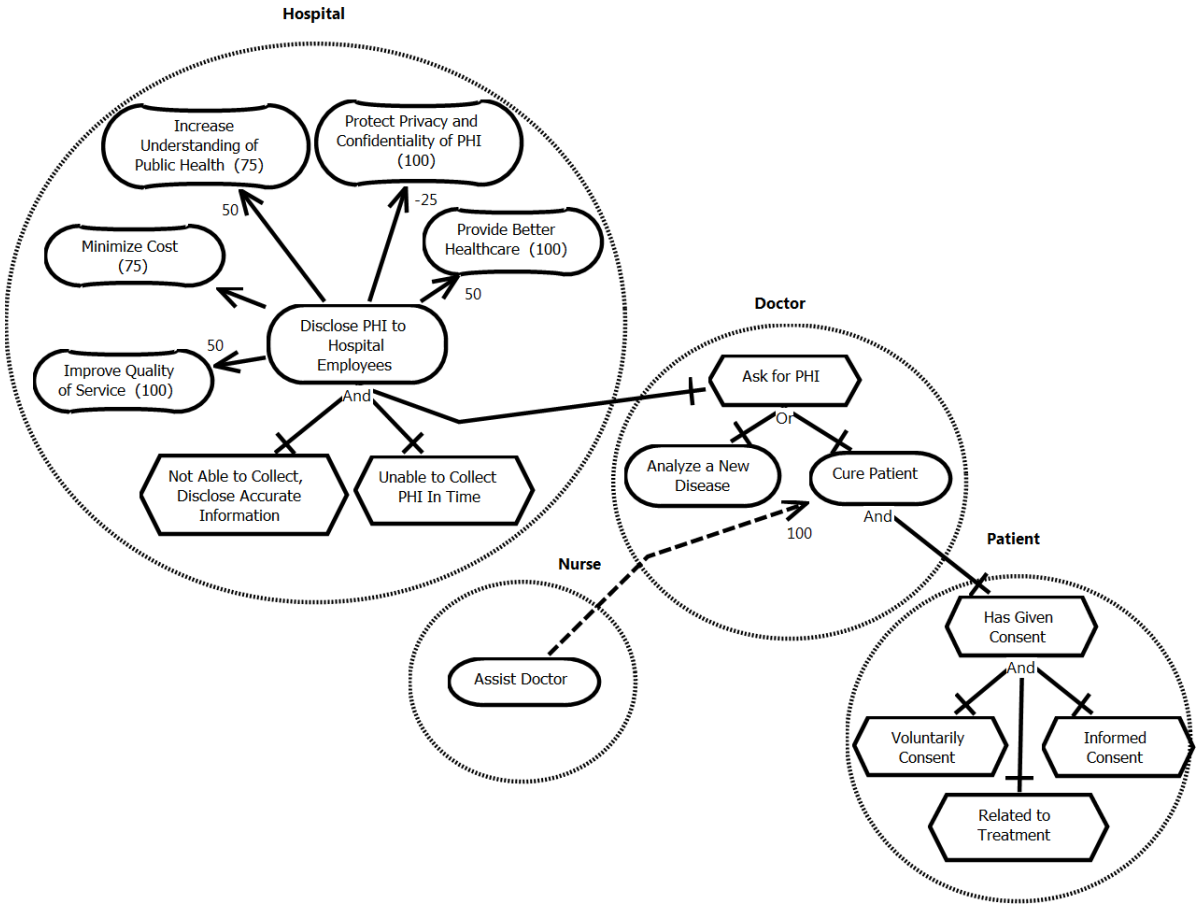

Figure 8.7: Hospital Model - Disclose to Hospital Employee - Modified

Note that there is no new business process created for these three new activities of the hospital. However, the business processes from the first case study in Chapter 6 are still valid here.

In the organization, this step is potentially done by a person playing the *business analyst* role.

8.7 Step 7 – Defining Consequence Goals and Model

We extend the consequence model of Section 6.6 (Figure 6.13) to also capture the consequence of non-compliance for the new regulations. Three consequences of non-compliance

were identified. These consequence goals, which are annotated with the «Consequence» stereotype, are Avoid Bad Reputation, Avoid Financial Penalties and Avoid Lawsuits.

Figure 8.8 illustrates the high-level goals of the legal model connected to these consequence goals through contribution links, which define the importance of each legal goal on the related consequence goals. The links from the related legal model to the «Consequence»goals have positive contributions. As mentioned before, if legal goals are fully achieved, then consequence goals get the value 0 (or "None") otherwise they get a value from −100 up to 0 (i.e., denied or weakly denied). To reduce the complexity of the model, we only show the consequence of non-compliance for the new softgoals of the Legal GRL models.

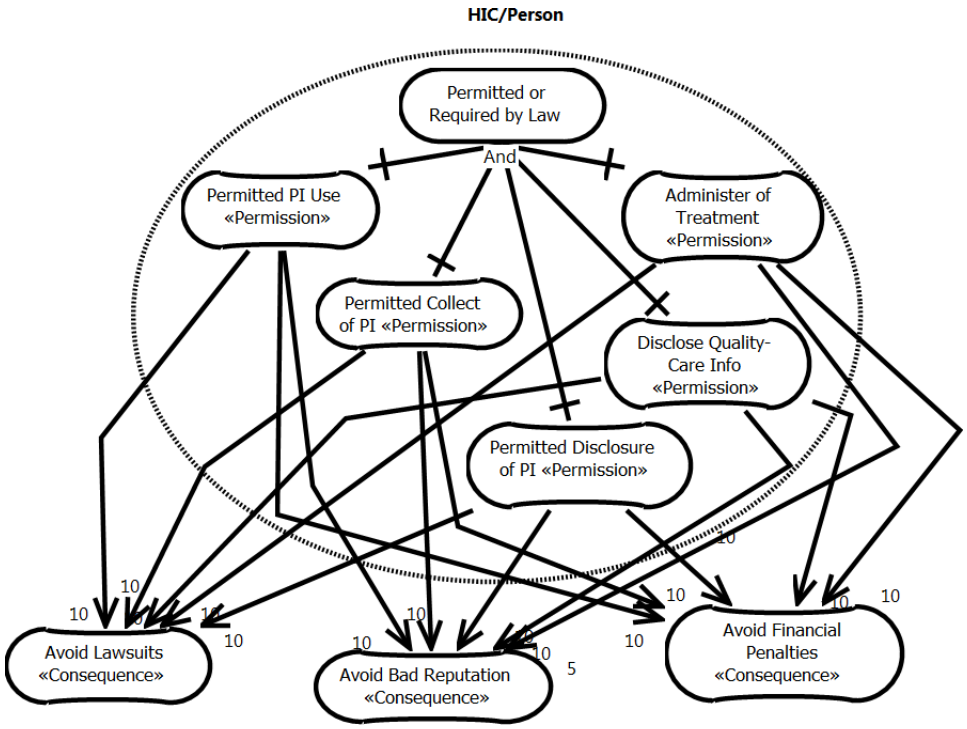

Figure 8.8: Extended Consequence Goal Model

8.8 Step 8 – Establishing Framework Links

After building the new models, we add typed URN links between the legal and organizational models. We connect the Hohfeldian model and GRL/UCM models through source links to their source documents, the GRL models to the Hohfeldian model through compliance links, and the UCM models to the GRL models via responsibility links.

We also connect the related parts of the Legal GRL models of the 4 regulations via traceability links. In Figure 8.11, for providing healthcare, all of the intentional elements in the bottom - right part of the figure that is related to consent as well as the actor have links to the intentional elements and actor of Article 18. For fundraising, Article 41 and 42 of FIPPA and Article 32 of PHIPA are complementary to each other. Figure 8.10 shows the correlation link between Article 32, Collect, Use or Disclose PHI for Fundraising and Article 42, For Fundraising Activities (FIPPA) with the main focus on Article 32. Figure 8.12 expands Article 42 of FIPPA and its links to the organization.

We also connected the new Legal GRL models to the organizational model through *weighted* and *simple* traceability links. Since the high-level organizational goals are similar to the first case study, the «Consequence»links remain the same.

Figure 8.9 and Figure 8.10 show partial views of the GRL models (i.e., Legal GRL, organizational GRL and consequence goals) for quality of care and fundraising activities of the hospital. Note that since this case study extends the previous case study, the views presented in the previous chapter are valid and remain similar; we only added to or extended the previous models. In the case where we were using the same models, for example Disclose PHI to Hospital Employees for treatment, we connected the same organizational model with additional information to the relevant legal models from this chapter (Figure 8.11).

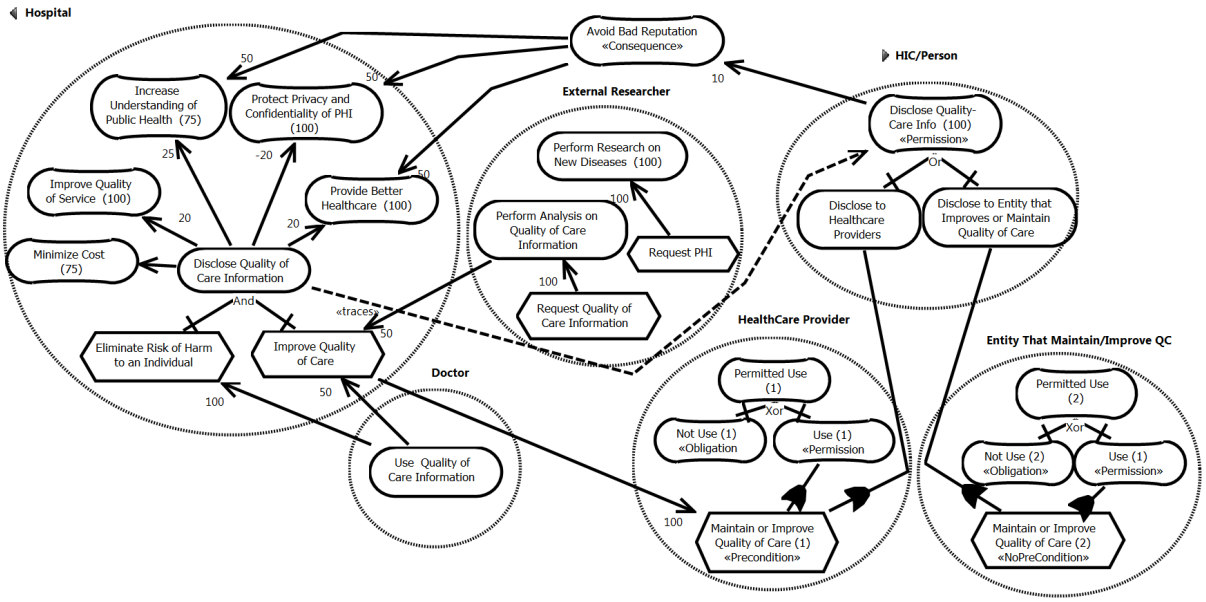

Figure 8.9: Legal - Organizational Model for Quality of Care

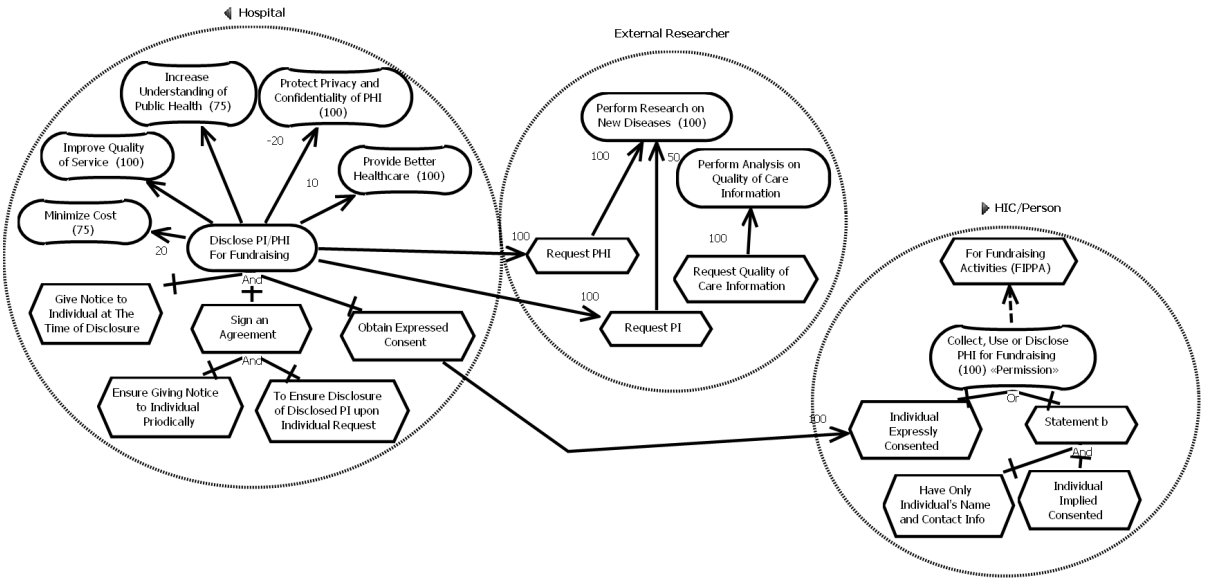

Figure 8.10: Legal - Organizational Model for Fundraising

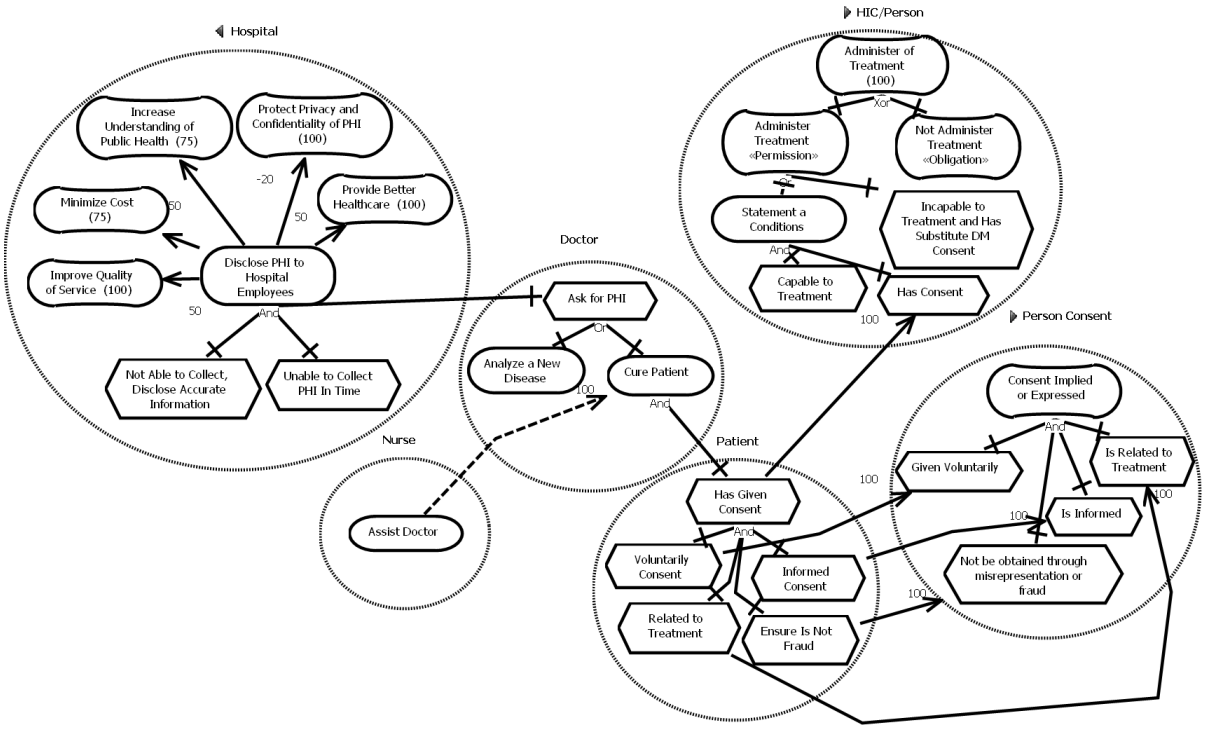

Figure 8.11: Legal - Organizational Model for Providing Healthcare

8.9 Compliance Analysis II

Similar to Chapter 6 and after extending the Legal URN model with the new regulations, we perform compliance analysis with respect to the steps identified in Chapter 5.

8.9.1 Steps A and B - Annotations and Links

In Step A, we annotate the intentional elements that are not relevant to the organization with «No» or «NoPreCondition». In Figure 8.9, the intentional element Maintain or Improve Quality of Care (2) gets tagged with «NoPreCondition» and in Figure 8.12 the intentional elements 42.a, 42.b, 42.c get tagged with «No».

In Step B, we annotate the links with their relevant stereotypes. In Figure 8.12, the link between Disclose PI/PHI for Fundraising and Permitted Disclosure of PI is annotated with «traces» and is shown as a correlation without any value.

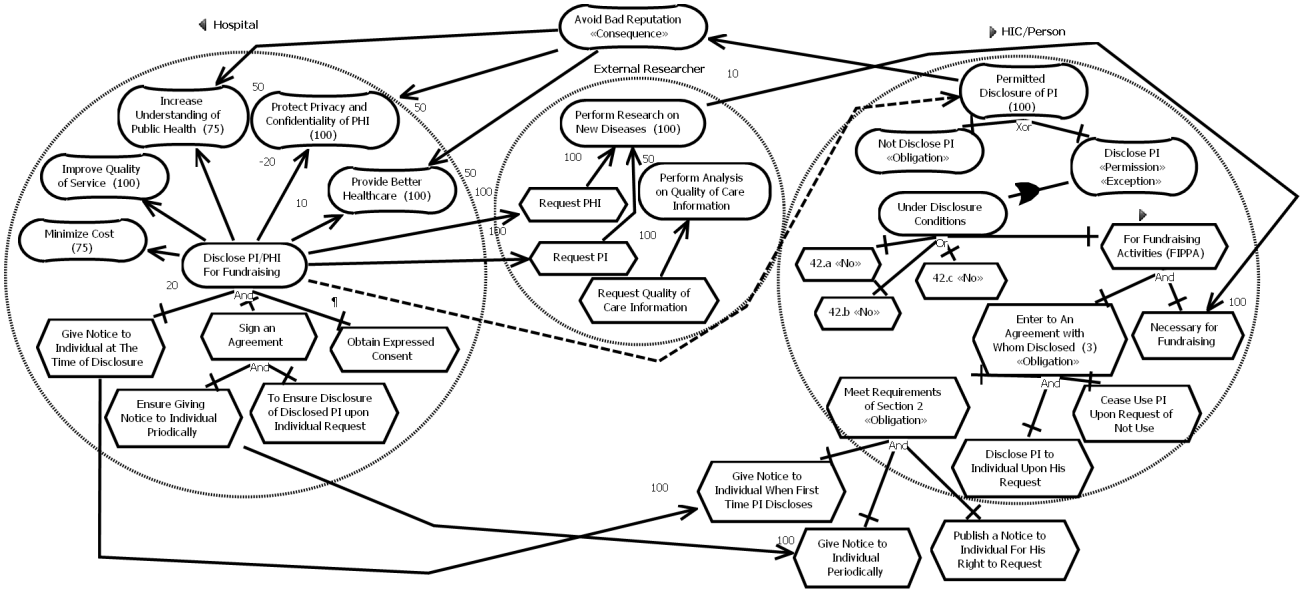

Figure 8.12: Legal - Organizational Model for Fundraising - Annotation

8.9.2 Step C - OCL Well-formedness Rules

We check the well-formedness of the combined model using the jUCMNav tool enhanced with our OCL rules. The result of this analysis is shown in Figure 8.13 and demonstrates the absence of well-formedness issues.

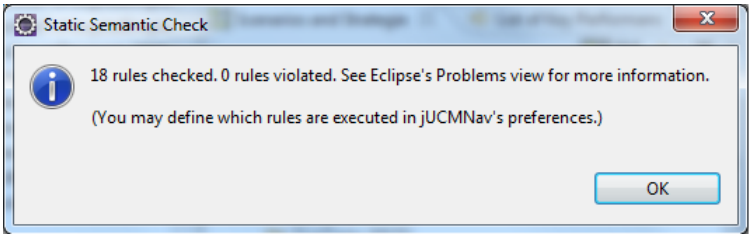

Figure 8.13: Result of Well-formedness Rules Checking

8.9.3 Step D - Quantitative and Qualitative Compliance Analysis (As-Is Strategy) – Bottom-Up Approach

In this section, we select a base strategy and illustrate the qualitative and quantitative compliance analysis techniques. We examine the degree of compliance of our organization to the parts of the regulations we identified and then detect non-compliant instances, if any.

Quantitative Analysis of Goal Models

For the quantitative analysis, we select a base strategy with quantitative satisfaction values for the organization's tasks. Similar to Section 6.8.3, we assume that the hospital performs its tasks completely and without any problem. Thus, these tasks get the value 100: Use Quality of Care Information, Request Quality of Care Information, Give Notice to Individual at The Time of Disclosure,Ensure Giving Notice to Individual Periodically,To Ensure Disclosure of Disclosed PI upon Individual Request,Obtain Expressed Consent,Voluntarily Consent,Related to Treatment,Informed Consent and Ensure Is Not Fraud.

Since the previous compliance analysis identified 5 non-compliant instances and prioritized them, those tasks are added to the model and also have satisfaction values of 100. Therefore, the compliance analysis only focuses on the new activities of the hospital.

The *weighted* traceability links between the two model are fully satisfied (100) as well. This means that if the hospital performs its task completely, it will contribute to and satisfy the target intentional elements of the legal model with the value 100, and otherwise that part of the law will not be fully satisfied.

In Figures 8.14 and 8.15, the tasks Publish a Notice to Individual for His Right to Request, Cease Use PI Upon Request of Not Use and Capable to Treatment are missing from the organizational GRL model. As a result, the high-level Legal GRL goals Permitted Disclosure of PI and Administer of Treatment are not satisfied and get a 0 value.

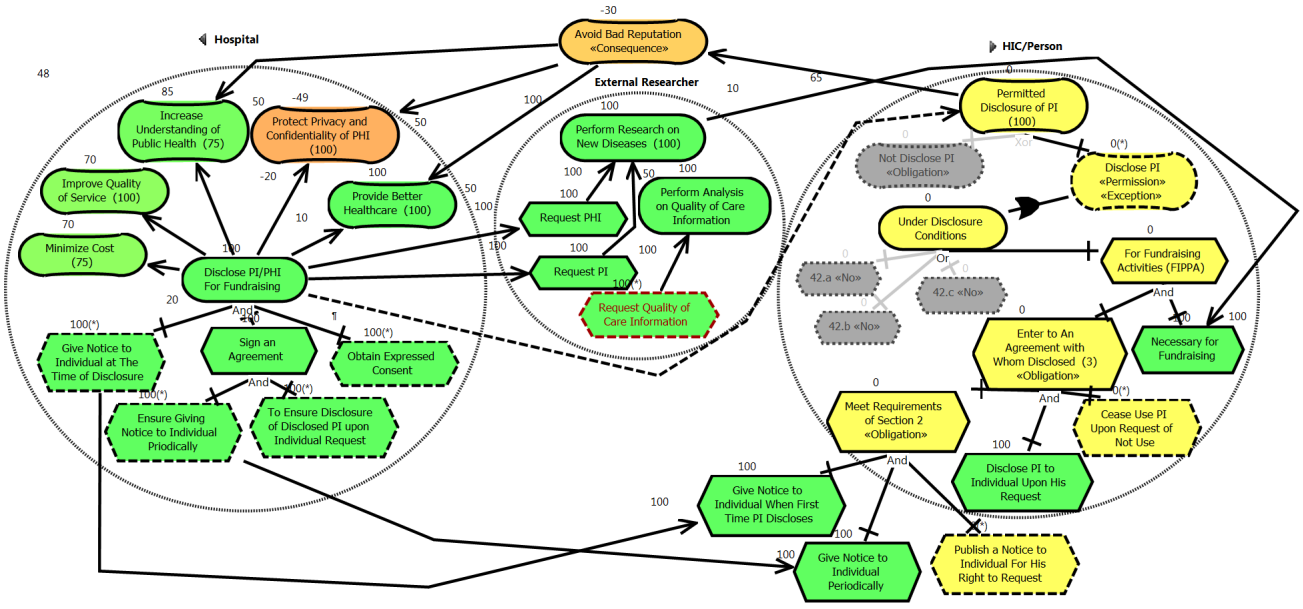

Figure 8.14: Quantitative Analysis of Organizational Model (1)

Figure 8.16 also presents the overall result of the satisfaction values of the Legal GRL model. Two softgoals Permitted Collect of PI and Permitted Disclosure of PI, which are related to fundraising activities, and the softgoal Administer of Treatment, related to disclosing to hospital employees, all get 0 as a resulting satisfaction level.

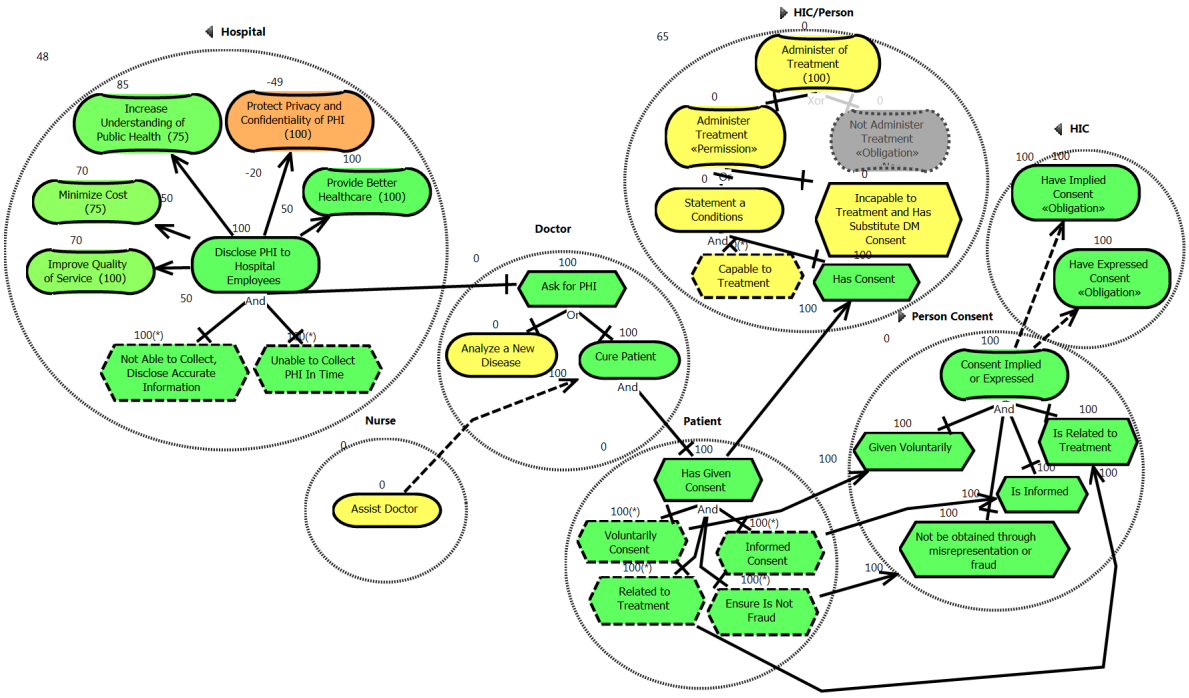

Figure 8.15: Quantitative Analysis of Organizational Model (2)

Since some of the high-level goals of the Legal GRL model have a satisfaction value of 0, the consequence goals get the value −30. These consequence goals are linked to the organization's softgoals. Figure 8.14 illustrates the satisfaction value for the organization's softgoals and the overall satisfaction value of the hospital. Only softgoal Provide Better Healthcare is fully satisfied whereas the other four softgoals of the organization have values inferior to 100: Increase Understanding of Public Health = 85, Minimize Cost = 70, Improve Quality of Service = 70 and Protect Privacy and Confidentiality of PHI = −49. As a result, the Hospital actor' satisfaction value is 48.

Qualitative Analysis of Goal Models

As an alternative approach to quantitative analysis (and to validate the second propagation algorithm), we repeat the analysis with qualitative values. Qualitative analysis is used normally when we lack the information needed to be confident about precise and small-grained values.

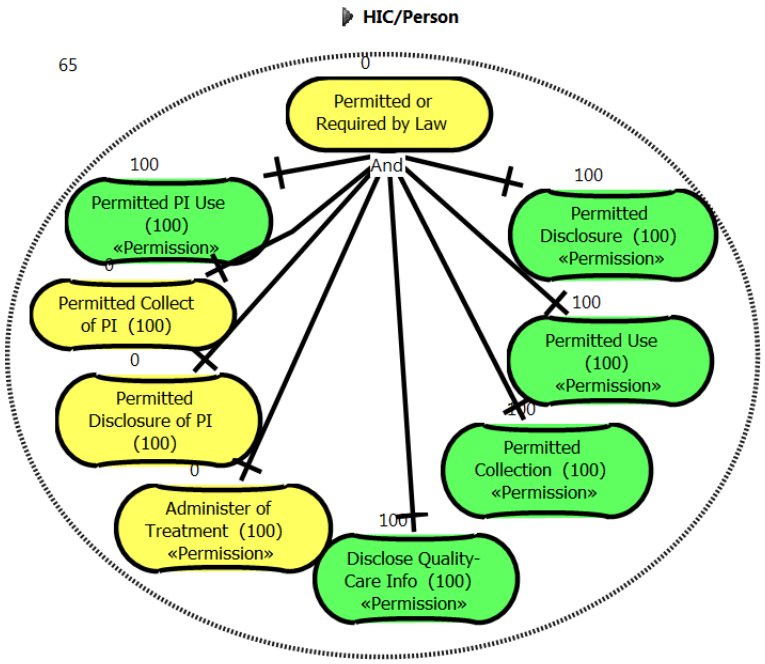

Figure 8.16: Quantitative Analysis of Legal GRL Model - High Level Goals

Similar to the quantitative analysis, we choose the base strategy by selecting all of the tasks of the organization (initializing them to a *satisfied* value) and propagating these values to the top-level goals of the organizational GRL model as well as the the Legal GRL model via *weighted* traceability links. These tasks are: Use Quality of Care Information, Request Quality of Care Information, Give Notice to Individual at The Time of Disclosure,Ensure Giving Notice to Individual Periodically,To Ensure Disclosure of Disclosed PI upon Individual Request,Obtain Expressed Consent,Voluntarily Consent,Related to Treatment,Informed Consent and Ensure Is Not Fraud. The *weighted* traceability links between the organizational model and the legal model have a *make* contribution value, which is the equivalent of the quantitative value 100. Thus, the satisfaction values of the organizational tasks are propagated to the legal tasks as-is. Figure 8.17 shows the qualitative analysis for the model of "Quality of Care". The legal softgoal Disclose Quality-Care Info is *weekly satisfied*.

Figures 8.18 and 8.19 present two other views of the whole model. The legal softgoals Permitted Disclosure of PI and Administer of Treatment have the value *none*, which is

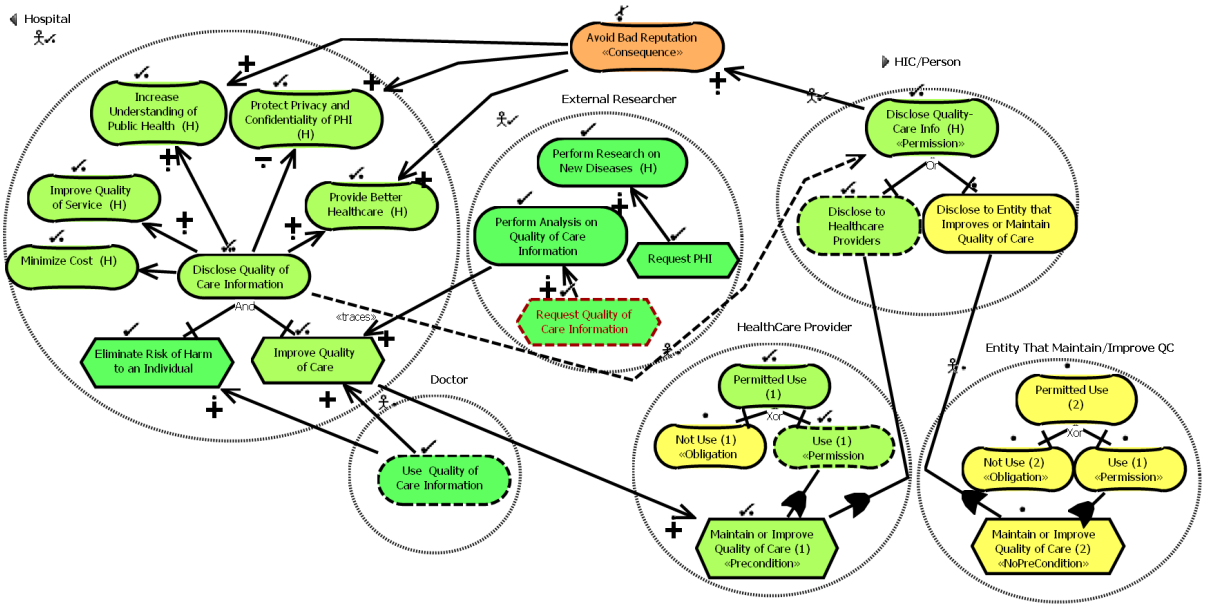

Figure 8.17: Qualitative Analysis of Organizational Model (1)

evidence of non-compliance. The tasks with no links to the organization model and the satisfaction value *none* are: Publish a Notice to Individual for His Right to Request, Cease Use PI Upon Request of Not Use and Capable to Treatment.

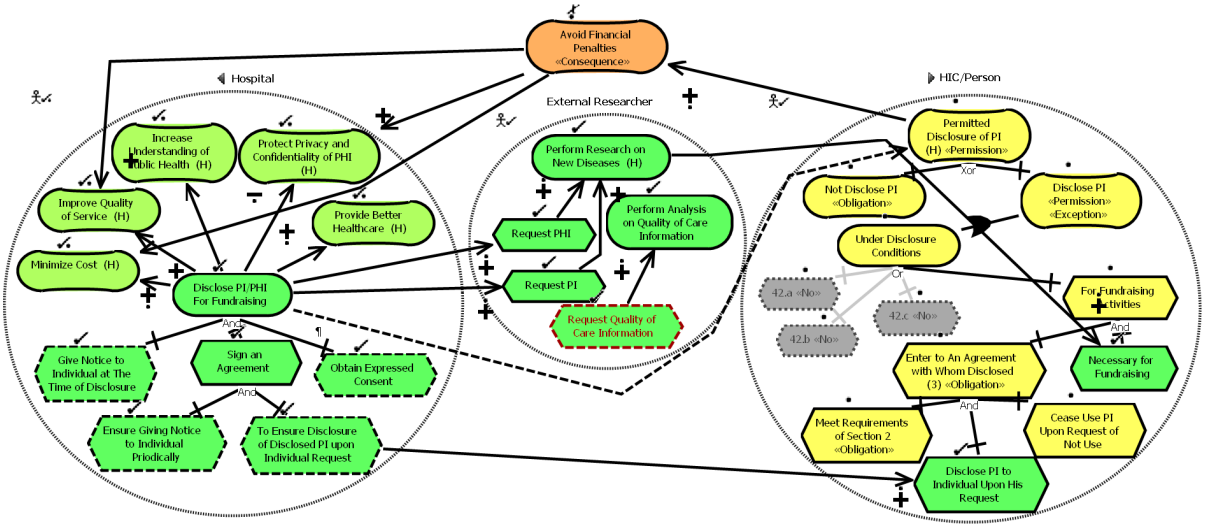

Figure 8.18: Qualitative Analysis of Organizational Model (2)

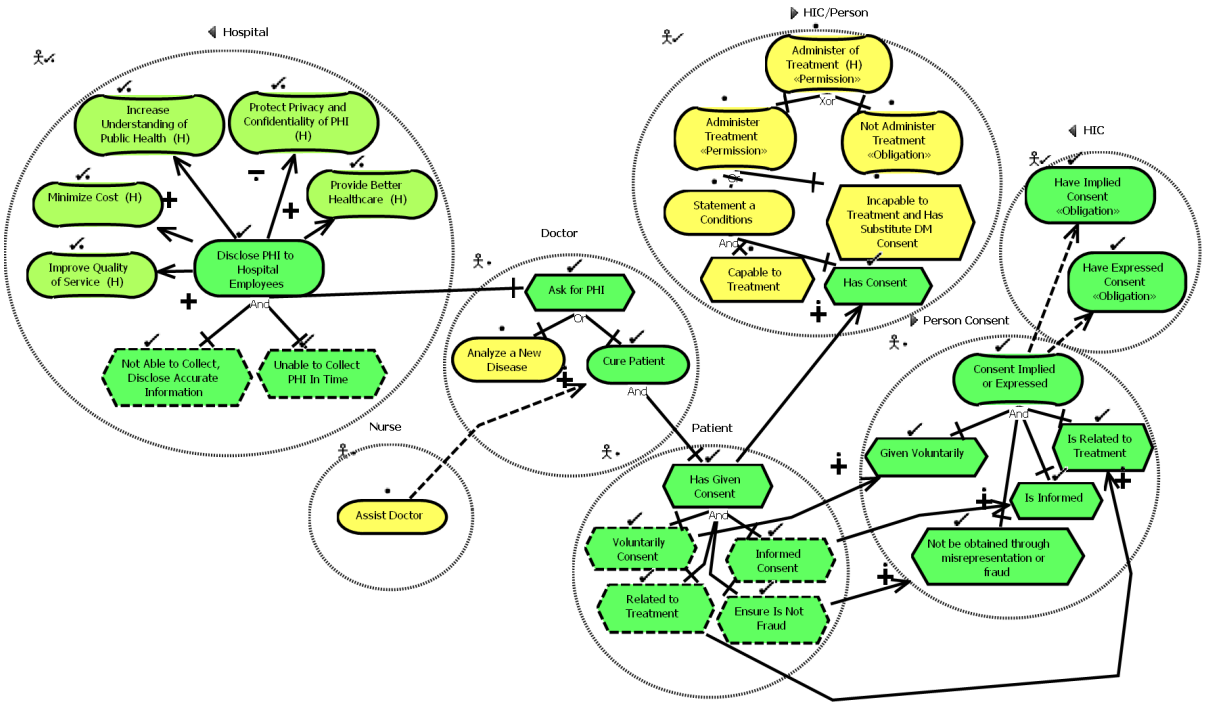

Figure 8.19: Qualitative Analysis of Organizational Model (3)

The consequence goals, which aim to illustrate the consequence of non-compliance on organizations, are *weakly denied*. Because of this negative effect, the high-level goals of the organization are not *satisfied*. Figure 8.19 shows the satisfaction value for the consequence goal Avoid Bad Reputation as well as for organization's softgoals and the overall satisfaction value of the hospital. All of the organizational softgoals and the hospital actor are *weakly satisfied*. The reason for getting a different result from the quantitative analysis algorithm is that the qualitative analysis algorithm deals with coarser-grained values and several levels of propagation may lead to results that are imprecise. However, even this evaluation helps identifying the non-compliant instances and their negative effect on organizational high-level goals.

8.9.4 Step E - OCL Compliance Rules Checking

After running the first strategy and getting the result of the compliance analysis (quantitatively and qualitatively), we run the OCL compliance rules (see Figure 8.20) to identify non-compliant instances. Three different rules are violated in total. In order to identify which rules are violated, we check the jUCMNav Problem view. Figure 8.21 provides the result of the compliance rule checking with 7 violation instances. 4 out of 7 violations are related to rule 20, 2 other ones are related to rule 19, and finally the last violation is related to rule 21. For example, the fifth violated rule in the list is related to rule 19 and it is located at "Enter to an Agreement with Whom Disclosed". This rule indicates that the "Obligation" goal must be evaluated to 100. However, as shown in figure 8.14, this goal is only evaluated to 0. Thus, this rule is violated at the location of the goal "Enter to an Agreement with Whom Disclosed".

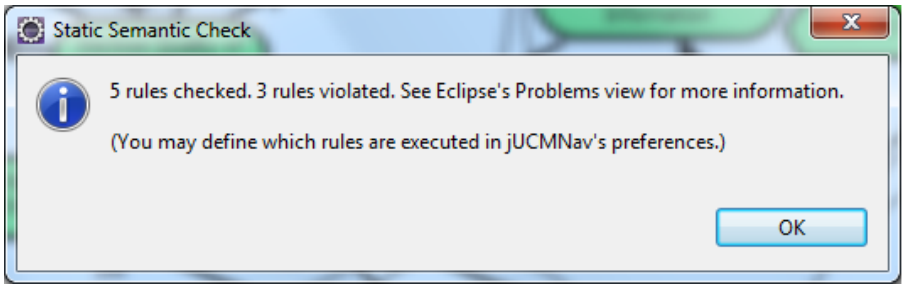

Figure 8.20: OCL Compliance Rules Analysis

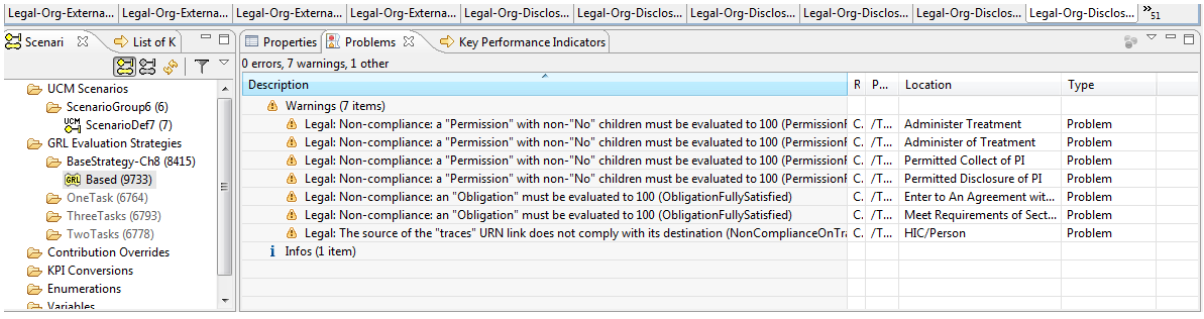

Figure 8.21: OCL Compliance Rules Result

Table 8.11: Result of the Strategies

	a	b	c	W1	OrgPr	W2	LegalPr	W3	CompPr	Priority
Strategy 1				0.35	48	0.35	65	0.3	100	69.55
Strategy 2	X			0.35	55	0.35	78	0.3	67	66.65
Strategy 3		X		0.35	48	0.35	65	0.3	67	59.65
Strategy 4			X	0.35	48	0.35	65	0.3	67	59.65
Strategy 5	X		X	0.35	55	0.35	78	0.3	33	56.45
Strategy 6	X	X		0.35	55	0.35	78	0.3	33	56.45
Strategy 7		X	X	0.35	48	0.35	65	0.3	33	49.45
Strategy 8	X	X	X	0.35	70	0.35	100	0.3	0	59.5

8.9.5 Steps F and G – What-If Strategies and Prioritization Algorithm

After determining the non-compliant instances, we prioritize them with the algorithm from Chapter 5. In the previous section, we identified three undecomposed tasks with satisfaction levels inferior to 100: a) Capable to Treatment, b)Cease Use PI Upon Request of Not Use and c)Publish a Notice to Individual for His Right to Request.

To prioritize these three tasks, we create new strategies that explore all combinations of 0 and 100 values for each of these tasks. The number of the strategies is $2^3 = 8$. As explained before, we compute the prioritization value Pr by using the following formula:

$Pr = \omega_1 \times OrgPr + \omega_2 \times LegalPr + \omega_3 \times ComPr$;

The OrgPr and LegalPr are extracted from the satisfaction values of the Hospital and HIC actors for each strategy, respectively.

We reuse the values from Chapter 6 for ω_1, ω_2 and ω_3. Thus, ω_1 and ω_2 are equal to 0.35 while ω_3 is equal to 0.3. We also use the same complexity analysis we did in that chapter. Hence, the strategy with no task gets a complexity value ComPr equal to 100, strategies with only one task get 67, 33 for two tasks, 0 for 3 tasks (the maximum). The result of this analysis (exported as a CSV file by jUCMNav) is shown in Table 8.11. In columns a to c, we indicate which tasks have been selected for the corresponding strategy.

According to the results, the best strategy is Strategy 2 (task (a) Capable to Treatment)

with a priority value of 66.65. The second best strategy is Strategy 8, with all three tasks. Assuming the task a is implemented, the third best strategies with 2 tasks that include a are Strategies 5 and 6, with the same priority value 56.45. With following these strategies, we can find the business process evolution path towards full compliance. First, the hospital has to ensure they have processes or activities to evaluate the capability of doing the treatment, next they have to modify their agreements for fundraising by adding activities supporting items b and c, in any order.

8.9.6 Evaluation of the Prioritization Algorithm

To validate the prioritization algorithm, we assume that the hospital implemented a set of activities to verify the capability of doing the treatment. Thus, the Legal task Capable to Treatment will be initialized to 100. We then repeat the quantitative compliance analysis and check this change with jUCMNav. Figure 8.22 shows the result of this analysis: the hospital and HIC/Person satisfaction values improve slightly from 48 to 55 and from 59 to 78 respectively. Table 8.12 also compares the satisfaction values of the hospital's softgoals for the base strategy and for Strategy 2.

Table 8.12: Hospital Softgoals Satisfaction Values - Comparison

	PBH	**IQS**	**PPC**	**IUPH**	**MC**
Base Strategy	100	70	-49	85	70
Strategy 2 Implemented	100	80	-40	90	80

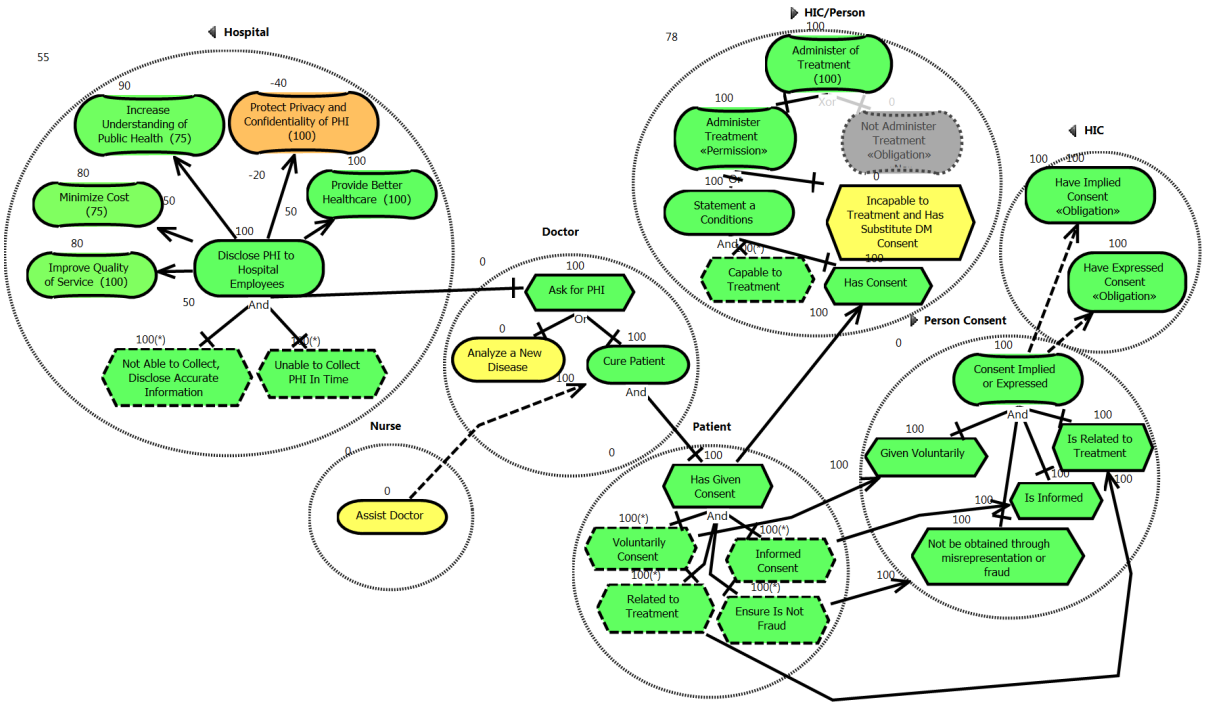

Figure 8.22: Quantitative Analysis - Task a Implemented

Running OCL compliance rules also gives us some improvement. The number of violations decreased from 7 to 5. Figure 8.23 illustrates this improvement.

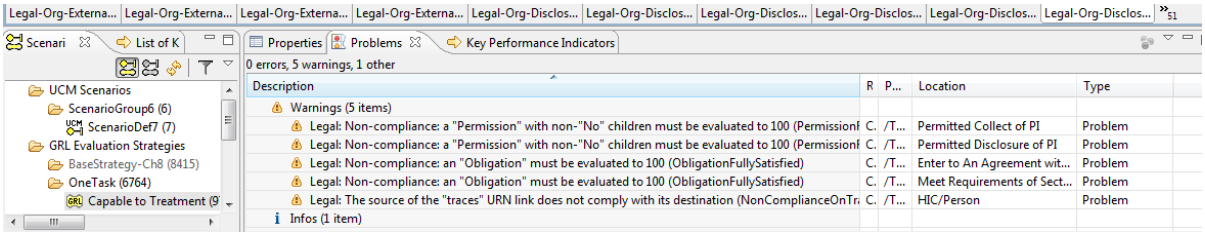

Figure 8.23: OCL Compliance Rules Result for Strategy 2

When we prioritize the two remaining tasks (Table 8.13), we notice that strategies that implement task b or task c have the same priority. In addition, since tasks b and c AND-decompose task (a) Enter to An Agreement with Whom Disclosed, implementing one of them does not improve the overall satisfaction value of either the hospital or the

Table 8.13: Result of the Strategies

	a	b	c	W1	OrgPr	W2	LegalPr	W3	CompPr	Priority
Strategy 1	X			0.35	55	0.35	78	0.3	100	76.55
Strategy 2	X		X	0.35	55	0.35	78	0.3	50	61.55
Strategy 3	X	X		0.35	55	0.35	78	0.3	50	61.55
Strategy 4	X	X	X	0.35	70	0.35	100	0.3	0	59.5

HIC/Person actor (i.e., the satisfaction values remain 55 and 78). Thus, to increase the compliance of the hospital to the regulations, the hospital needs to implement both tasks.

After implementing all of the tasks, the hospital becomes fully compliant with the modeled regulations. As Figure 8.24 shows, the HIC/Person legal actor is fully satisfied whereas the Hospital actor has satisfaction value of 70. All of the hospital's softgoals except Protect Privacy and Confidentiality of PHI are satisfied. When we check the OCL compliance rules, the tool also returns 0 rules violated (see Figure 8.25).

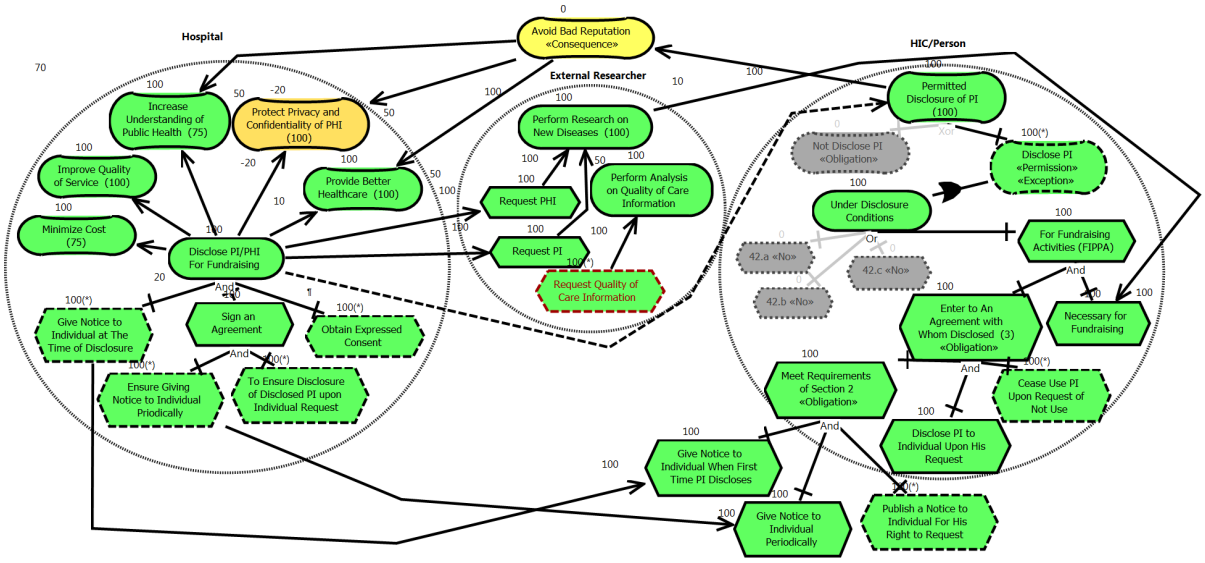

Figure 8.24: Quantitative Analysis - All Tasks Implemented

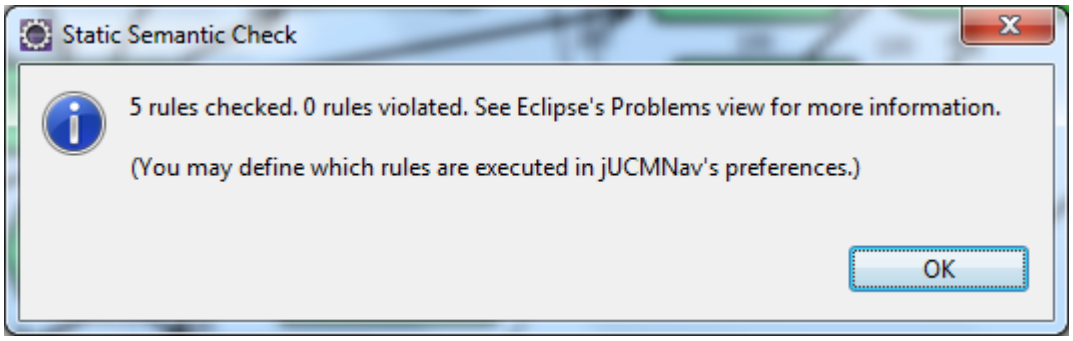

Figure 8.25: OCL Compliance Rules Result for All Tasks Implemented

8.10 Summary

In this chapter, we discussed a second case study, which is an extension of the first one. We identified three regulations and their relevant parts to our organization. First, we explained the new case study context and showed how to build its Legal model. Next, we provided a pair-wise comparison between the regulations and identified their conflicts and overlap. Then, we completed our models for the framework, provided the links, and verified their well-formedness. Finally, we performed quantitative and qualitative analysis of compliance and identified non-compliant instances. We prioritized these instances using our algorithm, implemented the first recommendation and evaluated our algorithms through this hypothetical situation. This chapter helped us evaluate our framework via another case study involving multiple regulations, some of which in areas different from privacy.

The next chapter further evaluates the validity of the framework through other assessments, discussions, and comparisons.

Chapter 9

Evaluation

In this chapter, we evaluate the LEGAL-URN framework and discuss its benefits and limitations. In Section 9.1, we first recall the general applications and benefits of the LEGAL-URN framework. In Section 9.2, we evaluate the framework by revisiting the gap analysis done during the systematic literature review. In Sections 9.3 and 9.4, we provide a comparison between the LEGAL-URN framework and two closely-related approaches based on URN: the plain URN framework itself (as a baseline) as well as Shamsaei' Indicator-based Policy Compliance Framework (ICPF). Then, we evaluate the framework via the results of the two case studies (Section 9.5) as well as through tool support (Section 9.6). Finally, we end the evaluation in Section 9.7 by discussing threats to validity.

9.1 Applications of the LEGAL-URN Framework

The LEGAL-URN framework's main objective is to provide organizations and their business analysts, compliance officers, and software engineers with a systematic approach to manage the complexity of regulations and of compliance. The framework can generally be used in different domains and for various situations in which organizations want to align their business objectives and processes with relevant (and evolving) regulations.

Furthermore, the LEGAL-URN framework is especially useful for organizations that need to comply with the same type of regulations in different jurisdictions, be it a healthcare service provider that must comply with legislation from different states in the USA, or a company with a presence in many countries (e.g., Google or IBM). In this case, handling multiple regulations can be harder since the regulations can overlap or conflict with each other.

Some of the benefits and features of the LEGAL-URN framework are recalled here:

- It uses the same modeling notation for both organizations and regulations. This helps organizations (including their analysts, engineers, lawyers, officers and managers) have a shared understanding of the regulations while enabling better comparisons between regulations and target business goals and processes.

- It promotes reuse across organizations in the same sector. Modeling the regulations with the Legal GRL and UCM models (including their traceability relationships) and annotating non-relevant parts of the model with «No» tags contribute to this reusability.

- It adds precision to URN models via stereotypes for intentional elements and links, accompanied with well-formedness rules, which implement the framework's metamodel, including deontic modalities derived from a Hohfeldian model.

- It includes quantitative and qualitative compliance analysis algorithms. On the one hand, qualitative analysis can be used when there is not so much information available about how well the organization can perform its tasks, with coarse-grained analysis results. On the other hand, quantitative analysis can provide more precise compliance results, but only if the organization has confidence in the quantitative values provided as input.

- The framework's prioritization algorithm can help organizations prioritize their instances of non-compliance based on high-level goals and on the consequences of

not satisfying high-level legal elements.

- The pair-wise comparison algorithm of Chapter 7, which takes advantage of a section-based clustering, makes it possible for organizations to take advantage of inter-regulation relationships to simplify the management of compliance with more than one regulation at a time.

- The framework comes with tool support for modeling, verifying, and analyzing compliance, and for efficiently prioritizing actions to address non-compliance.

9.2 Analysis Based on the Literature Review

In Chapter 3, we did a gap analysis to evaluate existing work against where we would ideally like to be in terms of compliance modeling and analysis. We identified a set of research questions and tried to answer them based on existing scientific literature. The main question and sub-questions asked in that chapter were as follows:

What ***goal***-oriented ***frameworks*** are there that help organizations establish their ***legal compliance*** and manage the ***evolution*** of their compliance?

1. Are there any ***goal modeling*** notations that support ***modeling legal*** aspects and support ***compliance***?

2. Are there any methods or frameworks that can ***integrate legal requirements*** with ***business processes*** to provide law-compliant business processes?

3. Are there any guidelines for ***extracting legal requirements*** and ***mapping*** them to goal models?

4. Are there methods that provide ***templates*** for ***modeling compliant business processes***?

5. Are there ***methods*** that help organizations ***prioritize*** instances of ***non-compliance***?

6. Is there any ***tool support*** for managing compliance?

At the end of Chapter 3, the systematic literature review helped conclude that none of the existing literature could address all of the issues discussed in the questions above. We identified several gaps between the existing literature and the needs of organizations, and categorized these gaps into five groups: RE/BP compliance framework, prioritization methodology, law-compliant BP templates, improved linking between legal and organizational models, and improved goal modeling notations and compliance analysis.

This thesis addressed these problems by developing the Legal-URN framework. In this section, we compare our work with existing literature qualitatively based on the five gaps previously identified. Table 9.1 summarizes the results of this comparison. Note that, in this table, we split the last group into two parts: modeling notations and compliance analysis. Note also that IPCF is not covered here as Section 9.4 will focus on that framework.

Based on the systematic literature review (and excluding IPCF), none of the RE frameworks for managing compliance puts together business and legal documents, goals, and business processes in a single framework. None provides a set of thorough guidelines on how to create legal models from legal documents, with mappings covering all aspects of the framework's concepts and meta-model. Our Legal-URN framework, on the other hand, contains four layers (including legal and organizational documents, Hohfeldian models, goal models, and business process models), distinguishes amongst different types of links between the framework's elements, captures consequence goals, and includes guidelines for extracting legal requirements models using GRL and UCM. It also manages change in goals, business processes, and regulations by building on previous work [23, 25] that exploits a commercial Requirements Management System (RMS) to maintain traceability.

In addition, the prioritization methodologies existing in the current literature [72] mainly focus on the complexity of legal statements and do not consider the impact of legal requirements on organizational objectives or the importance of instances of non-

Table 9.1: Qualitative Comparison between the LEGAL-URN Framework and the Literature

Problems	**LEGAL-URN Framework**	**Systematic Literature Review**
RE/BP Compliance Framework	4-layered framework including documents, goal models, business process models, traceability links between them, with construction guidelines and RMS-based change management	No concrete framework with guidelines
Prioritization Methodology	Based on legal and organizational high-level objectives as well as on the complexity of statements	Based on the complexity of statements only
Law-Compliant BP Templates	None	None
Improved Linking Between Legal and Organizational Models	Documents, goal models and business processes, but also between regulations	Not all aspects covered
Improved Goal Modeling Notations	Legal URN profile with stereotypes and OCL rules	Legal-specific goal modeling notations but no rule to check models
Improved Goal Modeling Compliance Analysis	Compliance-specific bottom-up quantitative and qualitative algorithms	Goal modeling analysis algorithm (bottom-up), not domain specific

compliance with respect to the law. The LEGAL-URN framework introduces a prioritization algorithm that considers all three factors for prioritizing instances of non-compliance.

In the existing literature, creating templates for law-compliant business processes has been tackled at a high level only, and the necessity of having such templates has been discussed. However, neither existing literature nor the LEGAL-URN framework are addressing this matter. It is necessary that, in future work, the LEGAL-URN framework gets extended by providing templates or samples to help organizations build compliant processes more easily. We have actually initiated some work in that direction [28, 29].

Although some existing frameworks from the literature put all of the right elements together, there is still a gap between extracted legal requirements and business processes,

especially in terms of impact. The LEGAL-URN framework provides guidelines on how to map legal requirements to Hohfeldian statements and then to Legal GRL models.

In the literature, there is work that extends existing goal modeling notations to capture aspects of the law. The *Nòmos* and *Nòmos* 2 frameworks [51, 100], SecureTropos, SI*, and GBRAM are some of these goal modeling notations. None of these includes all aspects of legal requirements (for example preconditions, exceptions, and cross-references) together with a domain-specific analysis algorithm and rules specific to legal compliance. However, the Legal GRL portion of the LEGAL-URN framework exactly maps parts of the legal requirements and statements to their equivalent concepts in GRL and identifies them with the help of a set of annotations (stereotypes). The framework also includes well-formedness and compliance OCL rules as well as improved quantitative and qualitative analysis algorithms used to address the requirements of the legal compliance analysis.

9.3 Comparison Between LEGAL-URN and Plain URN

In this section, we compare the LEGAL-URN framework with a compliance approach based on plain URN (e.g., standard URN, without any profile), as defined in Ghanavati's master's thesis [23]. For this comparison, we adopt and tailor the criteria for evaluating compliance management frameworks proposed by Kharbili et al. [57] and extend them with some additional criteria. The criteria defined by Kharbili et al. also focus on policies and regulations, and they are the only such criteria independently developed by others in the literature we surveyed. The list of criteria and their definitions are shown in Table 9.2.

Change Management: Both the LEGAL-URN framework and the URN framework are able to manage changes. They both include a set of links between all of the layers in their respective frameworks as well as between organizational and legal parts. This enables identifying any change in legal or organizational documents and their impacts on

Table 9.2: Evaluation Criteria for Compliance Management Framework

Criteria	**Definitions**
Change Management	The ability to handle changes and be able to track them in regulations or business processes.
Traceability	The ability to trace the organization's business processes, tasks or actions to regulations.
Complexity	The ability to deal with different levels of complexity, cover requirements of various legislations, and not be specific to one domain.
Efficiency	The ability to verify compliance and incorporate compliance checking algorithms.
Cost	The ability to reduce the cost of the compliance management.
Scalability	The ability to maintain the same level of efficiency for the framework no matter the size of the regulations or business processes.
Impact Analysis	The ability to capture the impact of changes of cross-referenced regulations on the business processes.
Accuracy of Models	The ability to verify whether the models are well-formed and correct.
Accuracy of Compliance Analysis	The ability to identify instances of non-compliance with a certain degree of accuracy.
Prioritization Capability	The ability to systematically prioritize instances of non-compliance.
Reusability	The ability to reuse legal models in different cases and organizations.
Handling of Multiple Regulations	The ability to incorporate more than one regulation in the legal models and identify the commonality and differences in the regulations.
Tool Support	Have tool support for modeling and analyzing compliance.

models and legal compliance. Both frameworks can also be integrated with a Requirements Management System in order to automate change tracking and management.

Traceability: There is a set of links (traceability, compliance, responsibility and source links) between the legal and organizational models in both the Legal-URN and URN frameworks. Via these links, it is possible to track the activities and tasks that exist in the organizational business processes, which are related to the regulations in both frameworks. This capability helps organizations to provide rationales about their regulation-related activities.

Complexity: The plain URN framework uses standard GRL and UCM models and it

does not distinguish between the different types of legal goals. It also does not contain the Hohfeldian layer to formalize the modeling and deal with the complexity that can exist in regulations. The LEGAL-URN framework includes the Legal URN profile for compliance which helps distinguish between various types of goals (such as obligations, permissions, exceptions, etc.). The Hohfeldian model layer of the LEGAL-URN framework is based on the Hohfeldian ontology for regulations, which enables the framework to handle many categories of regulations.

Efficiency: The LEGAL-URN framework adopts and extends the quantitative and qualitative GRL analysis algorithms and is able to calculate the degree of compliance of organizations with regulations automatically based on combinations of low-level intentional elements (tasks). In addition, with the compliance OCL rules, it is possible to identify violations of the regulations automatically. These capabilities are aligned with the efficiency criterion. The plain URN framework, however, does not include any quantitative or qualitative compliance analysis, nor does it include compliance violation detection rules. To identify any violation in the plain URN framework, it is necessary to identify missing links manually.

Cost: Creating Legal URN models is time consuming and requires much manual effort with both frameworks. However, once such models are available, they enable automatic compliance management. This can reduce the cost of future analyses and keep the cost of evaluating potential changes dramatically low. The LEGAL-URN framework is better than the plain URN framework in terms of cost as the former offers the capability of annotating non-relevant parts of the legal model with «No» tags and automatically remove them from compliance analysis. This feature makes legal models reusable (and tailorable) across several organizations that need to comply with the corresponding regulations.

Scalability: The URN standard, supported by jUCMNav, supports many scalability features. It is possible to split a large model across several views/diagrams and where the same model element is referenced many times. The analysis provides a single result

for the whole model, independently of the number of views/diagrams. Both frameworks take advantage of this feature. Also, many years of experience have demonstrated that goal-oriented analysis with jUCMNav can handle large URN models well [4].

Impact Analysis: With LEGAL-URN, cross-referenced statements are captured via «XRef» goals and are linked to their related statements through URN links. This helps capture changes in the cross-referenced model and identify their impact on the legal and organizational models. The URN framework does not support such impact analysis because it fails to distinguish between different goals and does not include cross-references.

Accuracy of Models: The LEGAL-URN framework is based on the Hohfeldian ontology and it provides a mapping between the concepts of the Hohfeldian model and the concepts of the Legal GRL model. In addition, well-formedness OCL rules can check the models to enforce the rules of the framework. These two features, which do not exist in the plain URN framework, contribute to the accuracy of the models.

Accuracy of Compliance Analysis: The plain URN framework cannot calculate compliance as any instances of non-compliance are identified only through missing links, independently of GRL evaluation strategies or propagation algorithms. In large models with several views, this manual activity can be tedious and error prone, and certainly not amenable to determining a path towards full compliance. In contrast, the compliance analysis method of the LEGAL-URN framework is semi-automatic and the instances of non-compliance can be found automatically by checking OCL rules. In addition, the compliance analysis can be either quantitative or qualitative.

Prioritization Capability: The LEGAL-URN framework has an algorithmic method that supports organizations in prioritizing their instances of non-compliance based on their goals as well as on the complexity of the tasks. This capability is missing in the plain URN framework.

Reusability: With the possibility of annotating the irrelevant parts of legal models with «No» tags in the LEGAL-URN framework, the model of the law can be made once

and reused in different organizations with different situations. The plain URN framework has limited reusability capabilities; if the organization changes, it is necessary to eliminate non-relevant parts of the law completely (and manually) before performing analysis.

Handling of Multiple Regulations: The LEGAL-URN framework has a methodology that handles multiple regulations based on a section-based, pair-wise comparison of Hohfeldian statements. The Plain URN framework does not deal with multiple regulations.

Tool Support: Both frameworks have tool support for modeling and compliance management. Detailed tool support is discussed in Section 9.6.

Table 9.3 summarizes the above comparison. It shows that the LEGAL-URN framework outperforms the Plain URN framework on nine criteria while the two are equivalent on the remaining four criteria.

Table 9.3: Comparison between Legal-URN and Plain URN

Criteria	**Legal-URN Framework**	**Plain URN Framework**
Change Management	Yes	Yes
Traceability	Yes	Yes
Complexity	Yes	Very limited
Efficiency	Manual strategies with automated compliance analysis	Entirely manual, through missing links
Cost	High creation cost, but with reusable legal models, and low analysis cost	High creation and analysis costs
Scalability	Yes	Yes
Impact Analysis	Yes (with XRef and URN links)	No
Accuracy of Models	Yes (stereotypes and well-formedness rules)	No annotations or model checking rules
Accuracy of Compliance Analysis	Automatic qualitative and quantitative analyses, with OCL compliance violation detection rules	Entirely manual, through missing links
Prioritization Capability	Yes	No
Reusability	Yes (must stereotype some elements)	Partially (must remove model parts manually)
Handling of Multiple Regulations	Yes (pair-wise comparison)	No
Tool Support	Yes	Yes

9.4 Comparison Between Legal-URN and IPCF

In this section, we compare the Legal-URN framework with the Indicator-based Policy Compliance Framework (IPCF) [97] based on the criteria defined in the previous section. IPCF, introduced in Chapter 3, is based on URN and combines policy and rule models together with models capturing business goals, business processes and their relative importance to the organization in order to measure compliance. IPCF uses indicators/KPIs (and a tailored quantitative algorithm based on [2])) for precise measurement, OCL rules for checking model well-formedness, and jUCMNav for tool support. Each criterion in this section focuses more on ICPF and does not necessarily repeat all that was described in the previous section for the Legal-URN framework.

Change Management: The LEGAL-URN framework is able to manage changes through the links that exist between all layers and the two models. IPCF, on the other hand, does not support change management automatically; links to source documents are particularly absent. However, it takes advantage of jUCMNav's support for hyperlinks to connect (unidirectionally) model elements to the corresponding parts of online regulations.

Traceability: The LEGAL-URN framework includes a set of different kinds of links between the legal and organizational models. IPCF supports this property partially through the linking of some GRL and UCM elements of the organization together.

Complexity: The LEGAL-URN framework exploits the Hohfeldian ontology as well as deontic modalities and other types of goal annotations, independently of the regulated domain. IPFC also contains a GRL profile to manage goal model families and to solve maintenance and ambiguity issues in models. The case studies used for IPFC demonstrate that this framework is domain independent.

Efficiency: The extended quantitative and qualitative GRL analysis algorithms of the LEGAL-URN framework support calculating the degree of compliance of organizations with the regulations automatically once manually (but rigorously) created strategies are provided. OCL rules detect compliance issues automatically. IPFC also includes a GRL propagation algorithm as well as OCL constraints to analyze compliance rules and detect non-compliance elements automatically. Manual strategies can be created to explore compliance improvements.

Cost: Similar to the LEGAL-URN framework, IPCF incurs a high cost for creating organization and regulation models with URN. In both cases, construction guidelines are provided, together with the possibility to tag the legal model in order to tailor it to a particular context (and possibly amortize the cost of the legal model construction over many organizations). They are hence similar in terms of cost.

Scalability: Both frameworks take advantage of existing URN and jUCMNav scalability features regarding large models and the handling of many strategies.

Impact Analysis: While LEGAL-URN uses «XRef» goals and URN links to manage cross-referenced statements, IPFC only uses the what-if strategy feature of jUCMNav to create as-is and to-be strategies and analyze the impact of a change on a policy, goal, or business processes. This capability of IPCF (which is also indirectly supported in LEGAL-URN) is semi-automated and prone to errors.

Accuracy of Models: A LEGAL-URN framework and IPCF both provide mappings between regulation meta-models and GRL, accompanied by OCL well-formedness rules. While IPCF adds indicators to models (which can be more precise than simple tasks and their satisfaction levels), it does not have any formal regulation ontology. Both of the frameworks still need legal models to be validated by legal experts.

Accuracy of Compliance Analysis: The LEGAL-URN framework includes automatic quantitative and qualitative compliance analysis algorithms and OCL compliance checking rules. It also considers the consequences of non-compliance on the satisfaction of the organization goals. IPCF uses indicators/KPIs with a quantitative algorithm for the compliance measurement and policy monitoring. The indicators can be fed by external sources of data, which improves accuracy of the analysis.

Prioritization Capability: The prioritization algorithm of the LEGAL-URN framework is based on the overall satisfaction of organizational goals, the overall satisfaction of legal goals, and the complexity of the tasks. The prioritization method in IPFC considers the importance of values of the rules as well as compliance levels.

Reusability: Both of the frameworks use «No» tags to eliminate the irrelevant parts of regulations or policies from analysis and support reusing the same legal models many times.

Handling of Multiple Regulations: While LEGAL-URN can handle multiple regulations, IPFC does not include any explicit algorithm or methodology for handling multiple regulations.

Tool Support: Both frameworks have the same tool support, namely jUCMNav.

Table 9.4 illustrates the summary of the comparison and the discussion. It highlights

that the LEGAL-URN framework clearly outperforms ICPF on four criteria (change management, traceability, impact analysis, and the handling of multiple regulations) and does slightly better than ICPF on two others (complexity and prioritization). However, ICPF does slightly better than LEGAL-URN on two criteria (the accuracy of models and of the compliance analysis), mainly because of the presence of indicators. The two frameworks are fairly equivalent on the remaining five criteria.

Table 9.4: Comparison between LEGAL-URN and IPCF

Criteria	**LEGAL-URN Framework**	**IPCF**
Change Management	Yes	Very limited
Traceability	Yes	Partially
Complexity	Yes	Yes (but without Hohfeldian and deontic modalities)
Efficiency	Manual strategies with automated compliance analysis	Manual strategies with automated compliance analysis
Cost	High creation cost, but with reusable legal models, and low analysis cost	High creation cost, but with reusable legal models, and low analysis cost
Scalability	Yes	Yes
Impact Analysis	Yes (with XRef and URN links)	Limited (to what-if strategies in jUCMNav)
Accuracy of Models	Yes (stereotypes and well-formedness rules)	Yes (stereotypes and well-formedness rules, with indicators but without deontic modalities)
Accuracy of Compliance Analysis	Automatic qualitative and quantitative analyses, with OCL compliance violation detection rules	Automatic indicator-based quantitative analysis, with OCL compliance violation detection rules
Prioritization Capability	Yes	Yes (but without considering task complexity)
Reusability	Yes (must stereotype some elements)	Yes (must stereotype some elements)
Handling of Multiple Regulations	Yes (pair-wise comparison)	No
Tool Support	Yes	Yes

9.5 Framework Evaluation Based on the Case Studies

In this thesis, we performed two case studies to evaluate the framework.

In the first case study, we selected Personal Health Information Privacy Act (PHIPA) and an Ontario hospital (based for the most part on a real hospital, but anonymized) with the main goals of improving healthcare, investigating a breach, and proceeding for payment.

In this case study, we analyzed 58 statements from PHIPA (including 28 Duty-Claim and 30 Privilege-Noclaim statements) and created the corresponding Hohfeldian model. We did not find any Power-Liability or Immunity-Disability statements among the ones we used for the case study, as there are few such cases statements in PHIPA and they were not relevant to our case study.

We created the organizational and Legal GRL/UCM models and established the links between the two. We ended up with a model comprised of 9 organizational-legal views and verified its well-formedness. Next, by analyzing the compliance of the organization to the law quantitatively and qualitatively, we identified 5 legal tasks that the organization was not performing. By evaluating 32 what-if strategies and the prioritization formula, we were able to prioritize instances of non-compliance.

In the second case study, we repeated the same process with three additional regulations and business processes. We identified 16 additional legal statements. We performed a pair-wise comparison between these statements and PHIPA and identified the different relationship cases. To avoid having an even larger case study, we only focused on comparing these three regulations with PHIPA and put aside the 3 other comparison combinations. However, if we wanted to ensure full compliance to all four regulations, we would need to perform the pair-wise comparison for the other combinations as well. We leave this as a future work.

We created 6 additional organizational-legal views in the model. Based on the quantitative and qualitative analysis algorithms and the OCL compliance rules, we discovered

3 instances of non-compliance that were prioritized through what-if strategies and the prioritization algorithm.

These two case studies helped us illustrated some of the benefits and limitations of the LEGAL-URN framework. The main observable benefits are:

- Having both organization and legal models with the same notation.
- Having guidelines and a rigorous methodology to create legal models.
- Being able to identify the degree of compliance for organizations quantitatively and qualitatively.
- Having a repeatable methodology to create models and exploit such a framework.
- Having a rigorous method to compare multiple regulations and model them in a single model.
- Being able to prioritize instances of non-compliance.
- Having combined models of multiple laws that can be reused by different organizations.
- Having a framework that scales to realistic business processes/objectives and to real and sizeable laws.

The main limitations based on the case studies are:

- Creating the models is time consuming and requires experts to verify them.
- The pair-wise analysis is also time consuming and can take many minutes per pair of statements.
- The prioritization algorithm is only efficient with a small number of instances of non-compliance, although this has not proven to be a problem here, and although the generation of all strategies is also automatable.

9.6 Tool Support Evaluation

jUCMNav is the best known tool for URN modeling and analysis. In order to support the LEGAL-URN framework, we implemented three different extensions in jUCMNav: support for the Legal URN profile's stereotypes (with metadata), an enhanced compliance analysis based on extended qualitative/quantitative GRL propagation algorithms, and the new OCL well-formedness and compliance checking rules presented in Appendix B.

Note that all the URN figures and analysis results shown in this thesis were produced with this extended jUCMNav (which is now publicly available as part of the normal jUCMNav distribution).

Stereotypes

jUCMNav supports the display of metadata attached to model elements as stereotypes (between «and») when the metadata's name is prefixed with 'ST_'. Stereotypes can be added, modified, and removed manually using jUCMNav's Metadate Editor (Figure 9.1).

However, to improve the effiency of the tagging process, contextual pop-up menus are now available to support pre-defined sets of stereotypes for specific types of URN model elements. For example, in Figure 9.2, the modeler can add or remove stereotypes specific to goals, or to actors (note that these two sets are different).

GRL Propagation Algorithms

The GRL qualitative and quantitative algorithms were extended (in a backward compatible way) to take advantage of the stereotyped elements of the Legal URN profile. For example, as shown in Figure 9.3, the new algorithms eliminate the intentional elements with «No» tags automatically from the analysis. Eliminated elements (and their children) are also grayed out.

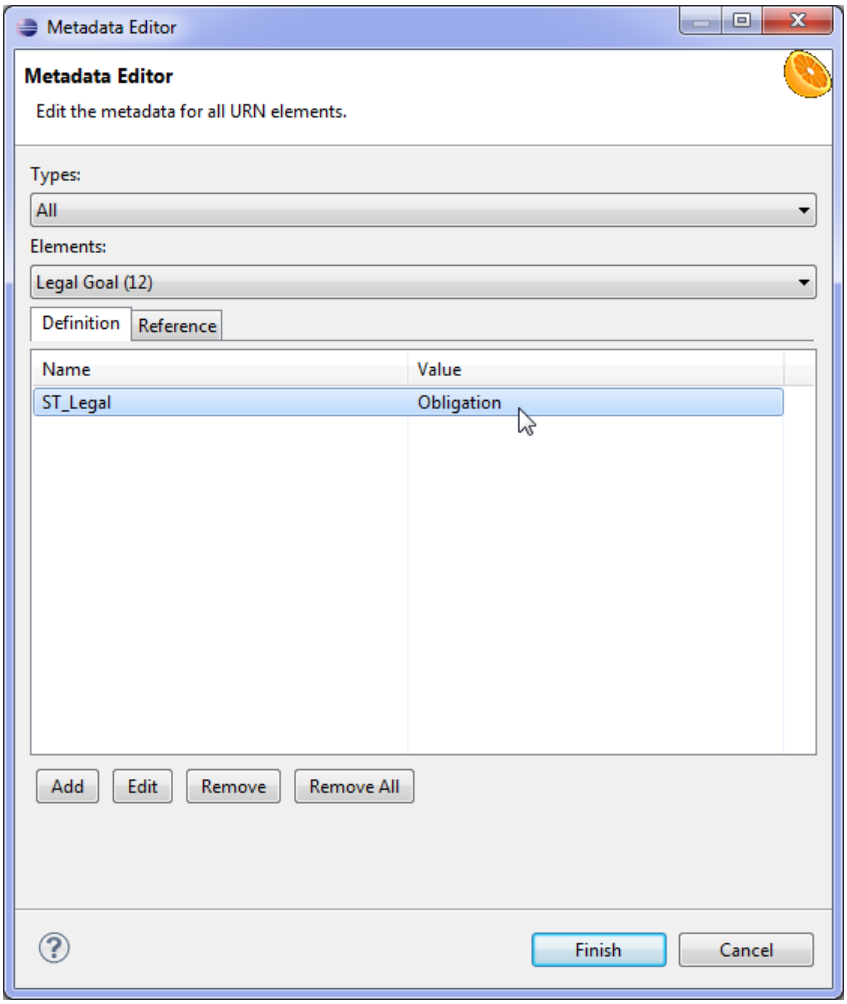

Figure 9.1: jUCMNav – Profile Stereotypes as Metadata

OCL Rules

The OCL well-formedness and compliance rules of the Legal URN profile are available in a new group of static semantic checking constraints in jUCMNav's preferences (Figure 9.4). These rules can be enabled, disabled, and checked at will, with violations reported in Eclipse's Problems view. The checking of these rules is basically instantaneous, even for large URN models.

This implementation and the case studies helped validate both the stereotyping approach and the OCL rules.

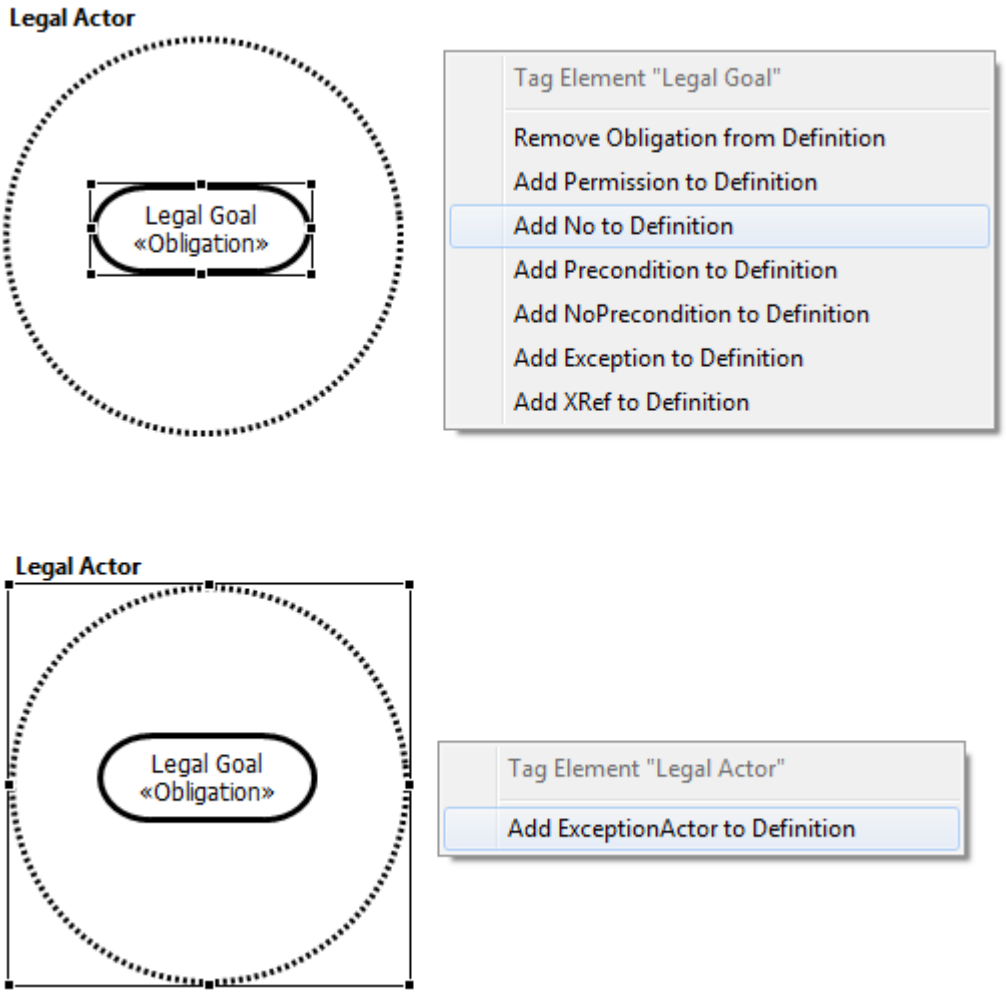

Figure 9.2: jUCMNav – Contextual Menus for Profile's Stereotypes

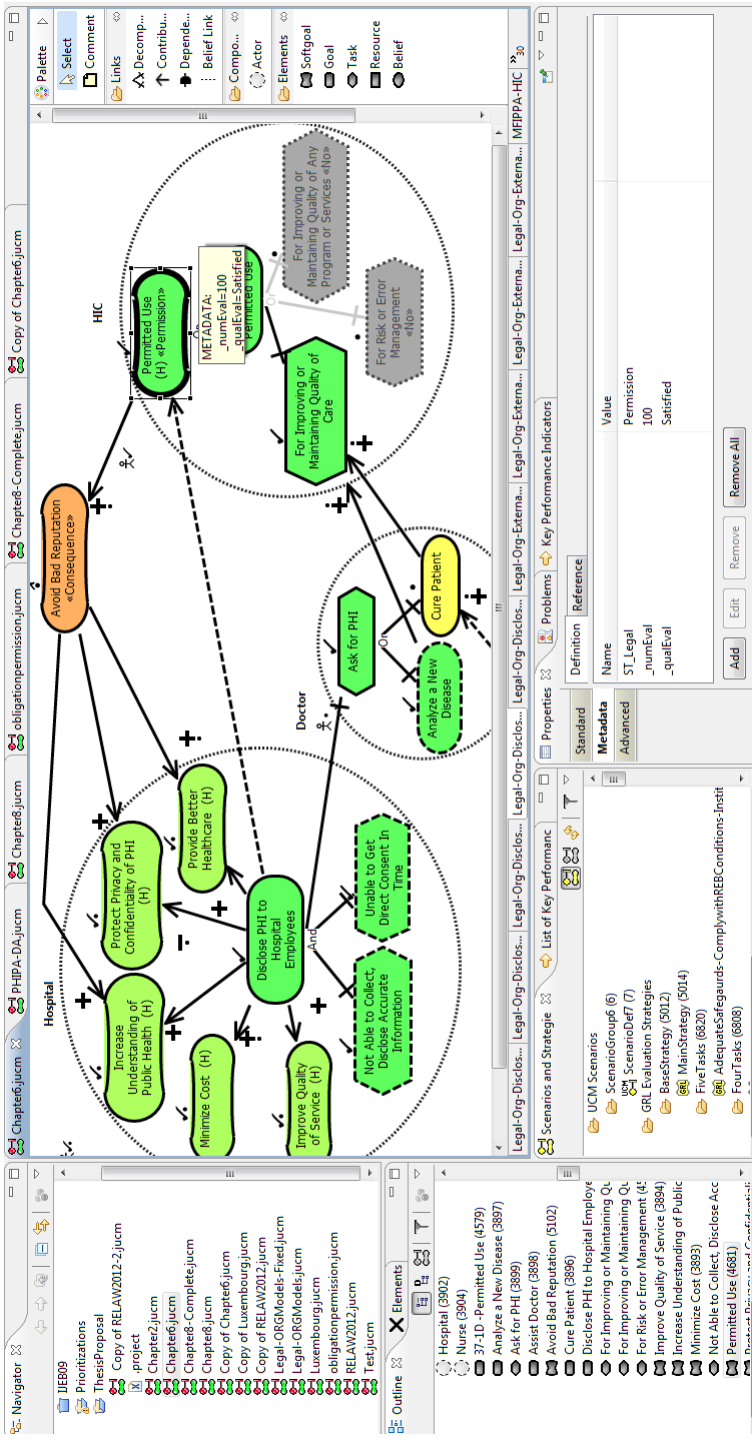

Figure 9.3: jUCMNav – Extended Analysis Algorithms

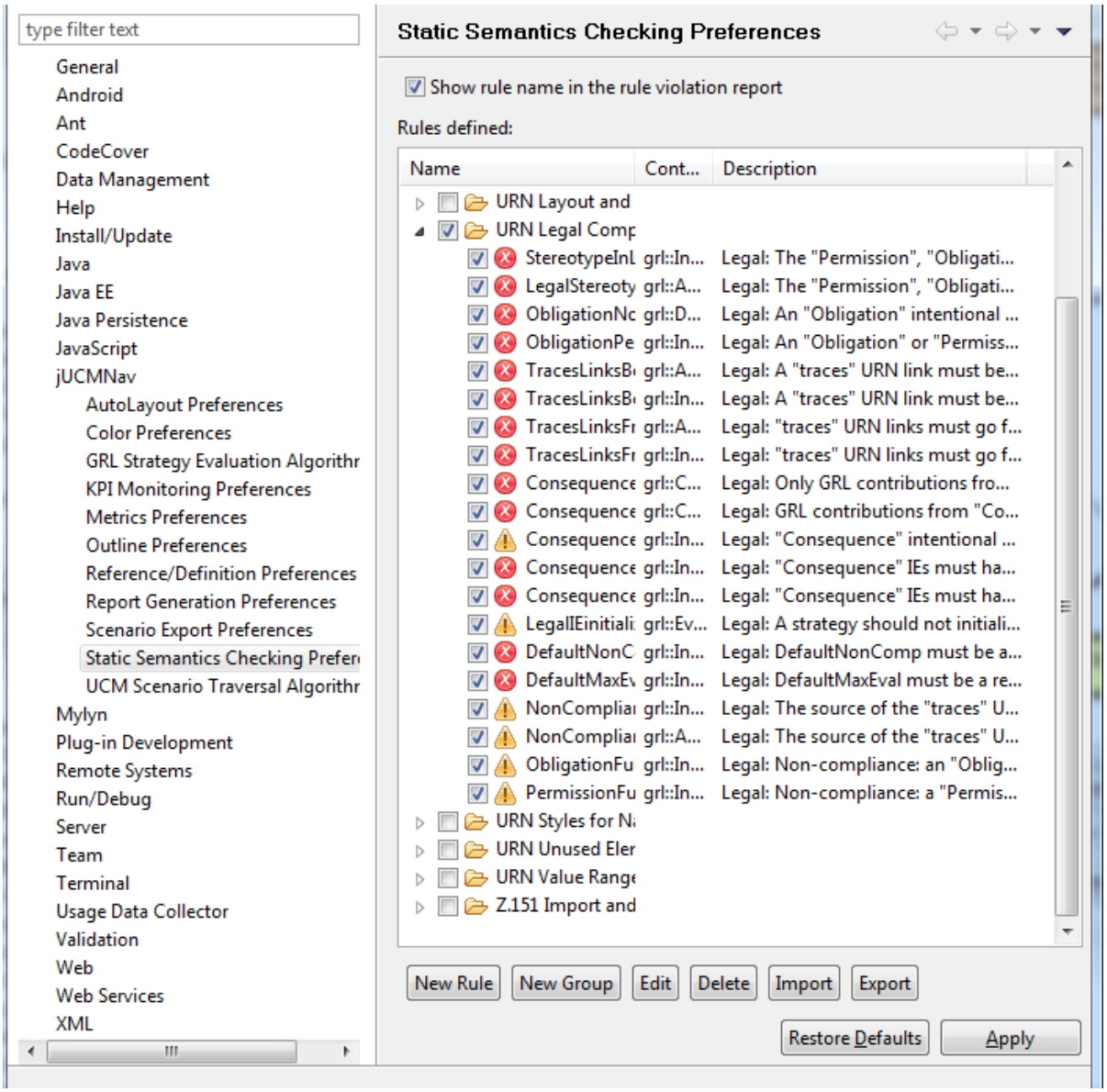

Figure 9.4: jUCMNav – OCL Rules for Legal URN Profile

9.7 Threats To Validity

In this section, we discuss the main threats to the validity of our framework based on the roadmap presented by Perry et al. [84], where they define three types of validity:

- **Construct Validity**: Examine to what extent the case studies actually measure answers to the questions
- **Internal Validity**: Examine any bias and other confounding factors
- **External Validity**: Verify the extent to which the results of the studies can be generalized.

Construct Validity

We designed and explored two case studies to validate the Legal-URN framework and verify if all of its steps could be realized. The first case study was constructed incrementally. In the first iteration, we did not have a very formal Hohfeldian model or very rigorous guidelines for creating GRL models. After modeling 10 articles from PHIPA, we identified the need for rigour. We created the meta-models for Hohfeldian models and Legal URN models, and provided mappings from the first type to the second. We also improved our OCL well-formedness and compliance rules as well as our compliance analysis algorithms to be consistent with our meta-models and guidelines. We modified the models in jUCMNav and added 8 more articles from PHIPA and verified their well-formedness. The results highlighted the model elements that were violating the well-formedness rules. We improved the guidelines and the models until we had no violations left. The objective of getting to a state without any violation in the context of one specific law was also identified as a threat. To mitigate this threat, we extended the framework and created a second case study, which helped validate the Legal-URN framework one more time with extended business processes and additional regulations different from PHIPA. In addition, we also evaluated our algorithm and method for pair-wise compar-

ison. First, we started by comparing the *Quality of Care Information Protection Act* with PHIPA, and defined the 6 pair-wise comparison cases. Next, we added *Freedom of Information and Protection of Privacy Act* to the model and compared it to PHIPA. Finally, the addition of the *Health Care Consent Act* was the final demonstration of the appropriateness of the approach. We eliminated the pair-wise comparison between QoCIPA-FIPPA, QoCIPA-HCCA and FIPPA-HCCA to reduce the size the case study. This elimination can be a threat to the validity of our compliance analysis result. However, due to the fact that the pair-wise comparison is actually optional and is only used to accelerate the creation of manual links between the organizational model and several legal models, this threat is fairly minor.

Internal Validity

Although, the case studies we used in the LEGAL-URN framework are based on the business objectives and processes of a real research hospital in Ontario (which is kept anonymous here), we never actually implemented the framework's recommendations in the hospital to understand the degree of practicality of the framework. All of the models were built by the thesis author, but they were verified by two reviewers, one of whom is a URN expert. Another threat to internal validity is that the contribution values as well as the complexity value ComPr and the weights (ω_i) in the priority formula were not validated by stakeholders. Different values will change the results of the compliance analysis. This could eventually be mitigated using some consensus-building approach such as the Analytic Hierarchy Process [92]. To further mitigate internal bias in the future, the models could be shared with legal experts as well as users (e.g., hospital employees) for validation. Usability studies involving requirements engineers, business analysts, lawyers, policy analyst, and compliance officers could also help to better validate the framework, especially in relation to the construction and understanding of the various models. Such usability studies will however be part of our future work.

External Validity

In order to mitigate the threat to external validity, we used four different regulations and six organizational business processes in our case studies. This helped illustrate that the Legal-URN framework is not simply specific to PHIPA and that it can be used for modeling other regulations too. However, the regulations we used in our work are all regulations that exist in Ontario and that are related to healthcare. We did not analyze our framework in other domains. To mitigate this threat, we used the Hohfeldian ontology to build the Hohfeldian models and Legal GRL models. The Hohfeldian ontology is a generic ontology for analyzing regulations and identifying different types of rights. Nevertheless, the framework needs to be further validated outside the healthcare area.

9.8 Summary

In this chapter, we evaluated the Legal-URN framework and discussed its benefits and limitations. First, we discussed the applications of the framework, and then we assessed its contributions against the gaps identified in our systematic literature review. Table 9.1 showed that the framework addresses most of the gaps, except the support for business process patterns. Next, we evaluated the framework based on an extended set of compliance management framework criteria and compared it with the Plain URN approach. Table 9.3 highlighted that our framework outperforms Plain URN on 9 out of 13 criteria, and both are equivalent on the remaining 4 criteria. A similar comparison was done with ICPF (Table 9.4). This time, the Legal-URN framework outperforms ICPF on 4 criteria, does slightly better than ICPF on 2 others, performs similarly on 5 criteria, and does slightly worse on the last 2 criteria (the accuracy of models and of the compliance analysis). We also summarized the benefits and limitations of the framework based on the two case studies, and discussed validation through tool support. Finally, we identified and discussed major threats to the validity of our work.

The next chapter will give general conclusions and present items for future work.

Chapter 10

Conclusions and Future Work

This chapter summarizes contributions of the thesis in Section 10.1 and discusses future work in Section 10.2.

10.1 Contributions

This thesis introduces a legal compliance framework called Legal-URN to help organizations extracting and modeling legal requirements, handling multiple regulations and analyzing compliance of their business processes and goals with regulations.

The thesis includes two major and several minor contributions. One of the major contributions of the thesis is the Legal-URN framework itself, consisting of four layers and two parts for legal and organizational models formalized using the same notation. These two views are connected to each other via a set of links that can be used to analyze compliance, manage change, and identify and prioritize non-compliance issues. This contribution has several sub-contributions, which are:

- A meta-model formalizing the concepts of the framework.
- Rigorous guidelines and mapping rules for extracting legal requirements from regulations and modeling them with URN. The Hohfeldian meta-model created for

LEGAL-URN maps exactly to the Legal GRL elements and is used to examine legal statements and extract the legal parts from regulations.

- Implementation of the meta-model with URN using a new Legal URN profile for compliance that includes specific stereotypes for intentional elements, links, and diagrams.
- Definition of the steps needed to build and exploit Legal URN models for compliance.
- Definition of a set of formal OCL rules for well-formedness and compliance checking.
- Improvement of the existing GRL quantitative and qualitative propagation algorithms for legal compliance analysis. These algorithms are also modified to eliminate legal elements tagged with a «No» stereotype from the analysis.
- Introduction of a methodology and a prioritization algorithm to help organizations decide in which order to handle instances of non-compliance.

The second major contribution of this thesis is a novel methodology for handling multiple regulations. This methodology, also part of the LEGAL-URN framework, has interesting characteristics:

- It entails modeling and analysis of 6 common cases that occur when trying to comply with multiple laws and regulations.
- It also introduces a new algorithm to perform pair-wise comparisons that makes use of a new <section> concept (added to our Hohfeldian meta-model) in order to drastically reduce the number of pairs of statements to analyze.
- Finally, the methodology provides guidelines that exploit the pair-wise comparison results to create reusable Legal GRL models and to link them to specific organizational models in a way that minimizes the number of manual traceability links required.

The other minor contributions of this work are:

- A systematic review of goal-oriented requirements management frameworks for business process compliance using 88 publications selected from five search engines and from the study of specialized conferences. This systematic literature review identifies gaps in the literature related to goal-oriented legal compliance frameworks and helps understand the needs and required future work in this field.

- Extension of the jUCMNav tool to support the new domain-specific URN customizations (Legal URN profile) for compliance, as well as the OCL well-formedness and compliance checking rules, and the new GRL analysis algorithms.

- Two case studies conducted to evaluate the feasibility, benefits and limitations of the Legal-URN framework. The second case study is the only one available, to our knowledge, that uses a goal-oriented compliance modeling approach to explicitly handle multiple regulations.

Together, all of the above contributions help answer the four questions raised in the research hypothesis (Section 1.2). In particular:

1. Chapter 4 describes how to extract (via a Hohfeldian model) relevant legal models (in our profiled URN) from source documents. This was further validated using four different laws in the case studies.

2. Chapter 5 explains how organizations can ensure their business processes and goals are compliant with legal documents.

3. Section 5.6 provides tool-supported algorithms to identify and prioritize instances of non-compliance, which also help find a proper balance between the organization goals and those of laws.

4. Chapter 7 provides a methodology that handles multiple laws.

10.2 Future Work

Future work for this thesis can be broadly grouped into the following categories:

- Support indicators in the LEGAL-URN framework. Indicators are now part of the most recent version of the URN standard, and their value for improving the precision of models and of compliance analysis was demonstrated in the Indicator-based Policy Compliance Framework [97].

- Add business process patterns to the LEGAL-URN framework. This gap, identified in the literature survey, is still unadressed by the framework. Such patterns would complement the Hohfeldian model and could be used as a starting point for building or completing organizational business processes. Some preliminary work has been done for creating such patterns [29, 28].

- Improve the priority formula, which is based on three factors: OrgPr, LegalPr and ComPr. The values of factors OrgPrand LegalPr are derived automatically from jUCMNav, but the factor ComPr is defined based on the number of tasks needed to be supported in each strategy. This approach is very simplistic since it could be possible that implementing a single task be more complicated than supporting two other tasks. In the future, it is necessary to explore the ComPr factor in more detail and create a method to define the values for this factor more precisely.

- Do prioritization based on top-down or constraint-based analysis algorithms. In order to avoid having to deal with a large number of what-if strategies, a new prioritization algorithm that tailors Luo's constraint-oriented evaluation algorithm [70] could be explored and implemented. This algorithm would replace the what-if strategies and directly identify the legal tasks that need to be implemented in order to optimize the priority formula, which balances organization satisfaction with compliance level and implementation effort.

- Develop a deterministic algorithm for pair-wise comparison of statements from different regulations. In this thesis, we identified 6 cases based on the pair-wise comparison method. To improve this comparison and formalize it in a better way, we aim, in the future, to replace the tables with a deterministic algorithm (or simply a decision tree) which can help identify the different cases and select appropriate modeling measures.

- Develop tool support to partially automate the deterministic pair-wise comparison algorithm, in order to reduce the current comparison effort.

- Perform a usability study for the Legal-URN framework with a group of legal experts, compliance officers, policy and business analyst, as well as requirements and software engineers. The usability study could be divided into five parts. In the first part, the framework and the necessary background knowledge are explained and then four experiments are conducted:

  - First experiment: Manual compliance analysis of a set of business processes with a piece of regulation.
  - Second experiment: Compliance analysis of a set of business processes with a piece of regulation based on the Legal-URN framework, with tool support.
  - Third experiment: Managing change in regulations and business processes, identifying the impact of such change and performing the necessary modifications, with tool support.
  - Fourth experiment: Adding another regulation and new business processes and performing the compliance analysis together with the algorithms for handling multiple regulations.

- Repeat the thesis' second case study with the complete pair-wise comparison combinations, evaluate and compare the results with the result of second case study of

this thesis and identify any potential risk or threat the case study introduced in our research.

- Integrate the measurement-oriented comparison of multiple regulations with GRL. Rifaut et al. [88] performed preliminary work on the design of new methods to analyze regulatory impacts on business operations based on the combination of Goal-Oriented Requirements Engineering (GORE) and Measurement-Oriented Requirements Engineering (MORE) techniques. The approach focuses on comparing and analyzing multiple regulations at different levels (i.e., national and international). This work would take advantage of the LEGAL-URN framework and combine it with a measurement framework [86].

Appendix A

Systematic Literature Review Documents

This appendix contains the titles of the papers selected from 11 sources (including five search engines) during the systematic literature review presented in Chapter 3. The main category is also indicated for each paper.

Table A.1: Papers Selected from ACM

Title	**Categories**
Organizational aspect of trusted legally valid long-term electronic archive solution	Goal Modeling
Preparing information security for legal and regulatory compliance (Sarbanes-Oxley and Basel II)	Others
Towards a framework for tracking legal compliance in healthcare	RE Framework
Towards a compliance support framework for global software companies	RE Framework
Managing the Alignment between Business and Software Services Requirements from a Capability Model Perspective	RE Framework
Mining and analysing security goal models in health information systems	Legal RE Extraction
Designing Law-Compliant Software Requirements	Goal Modeling
Compliance aware business process design	BP Compliance

Table A.2: Papers Selected from Scopus

Title	**Categories**
Policy-enabled goal-oriented requirements engineering for semantic business process management	Goal Modeling
Compliance analysis based on a goal-oriented requirement language evaluation methodology *(my work)*	Goal Modeling
A distributed requirements management framework for legal compliance and accountability	RE Framework
Comparative analysis between document-based and model-based compliance management approaches	Others
Regulatory compliance in information systems research - Literature analysis and research agenda	Literature Survey
A meta-model for modelling law-compliant requirements	Goal Modeling
Modeling, analyzing and weaving legal interpretations in goal-oriented requirements engineering	Goal Modeling
Personalized systems need adaptable privacy statements!: How to make privacy-related legal aspects usable and retraceable	Others
From laws to requirements	Legal RE Extraction
Requirements and compliance in legal systems: A logic approach	RE Framework

Table A.3: Papers Selected from Springer

Title	**Categories**
Towards a Framework to Elicit and Manage Security and Privacy Requirements from Laws and Regulations	RE Framework
Emerging Challenges in Information Systems Research for Regulatory Compliance Management	Literature Survey
A framework to support alignment of secure software engineering with legal regulations	RE Framework
Compliance in e-Government Service Engineering: State-of-the-Art	Literature Survey
A Requirement Engineering Framework for Electronic Data Sharing of Health Care Data Between Organizations	Others
On the Risk Management and Auditing of SOA Based Business Processes	BP Compliance
A Legal Perspective on Business: Modeling the Impact of Law	BP Compliance
Compliant Business Process Design Using Refinement Layers	BP Compliance
Compliance Requirements for Business-process driven SOAs	BP Compliance
Business Process Design as the Basis for Compliance Management, Enterprise Architecture and Business Rules	BP Compliance
Managing Legal Texts in Requirements Engineering	Legal RE Extraction
Establishing Regulatory Compliance for Information System Requirements: An Experience Report from the Health Care Domain	Goal Modeling
Model Based IT-Governance Compliance Analysis	Others
Legal compliance by design: technical solutions for future distributed electronic markets	BP Compliance
Evaluating existing security and privacy requirements for legal compliance	Prioritization, Legal RE Extraction

Table A.4: Papers Selected from IEEE Xplorer

Title	**Categories**
Modeling and Analysis of Laws using BPR and Goal-Oriented Framework	Goal Modeling
Early Studies in Acquiring Evidentiary, Reusable Business Process Models for Legal Compliance	RE Framework
Using Goal-Oriented Requirements Engineering for Improving the Quality of ISO/IEC 15504 based Compliance Assessment Frameworks	Goal Modeling
Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology	Others
Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act	BP Compliance
Governance Requirements Extraction Model for Legal Compliance Validation	Legal RE Extraction
Industry trends in business process management: getting ready for prime time	Others
Developing Production Rule Models to Aid in Acquiring Requirements from Legal Texts	Legal RE Extraction
Addressing Legal Requirements in Requirements Engineering	Literature Survey
Checking Existing Requirements for Compliance with Law Using a Production Rule Model	RE Framework
Towards a framework for law-compliant software requirements	Goal Modeling
User-centric Privacy Framework: Integrating Legal, Technological and Human Aspects into User-Adapting Systems	Others
A method to acquire compliance monitors from regulations	RE Framework

Table A.5: Papers Selected from Google Scholar

Title	**Categories**
A Business process Based Modelling Extension for Regulatory Compliance	BP Compliance
A Semantic Framework for Compliance Management in Business Process Management	BP Compliance
A Method for Identifying Software Requirements Based on Policy Commitments	Legal RE Extraction
On the use of the Goal-Oriented Paradigm for System Design and Law Compliance Reasoning.	Goal Modeling
Towards a framework for semantic business process compliance management	BP Compliance
Modelling security goals in business processes	Others
Governance Requirements Extraction Model for Legal Compliance Validation	RE Framework
Semantic Compliance Management in Business Process Management	BP Compliance
Architecting and Managing Virtual Learning Networks: A Business Process-orientated Approach to Legal Compliance	Others
Integrating business strategies with requirement models of legal compliance	BP Compliance
Validating Existing Requirements for Compliance with Law Using a Production Rule Model	Legal RE Extraction
Security and Compliance in Clouds	Others
A requirements management framework for privacy compliance	RE Framework
Towards legal programming: The incorporation of legal criteria in software agent design-Current proposals and future prospects	Others
Hints on how to face business process compliance	BP Compliance
Leveraging Goal Models and Performance Indicators to Assess Health Care Information Systems	Others
Legal Patterns Implement Trust in IT Requirements: When Legal Means are the	Goal Modeling
Law, Metadata and Semantics	Others
Validating Compliance with Privacy Legislation	RE Framework
Towards secure legally valid long-term electronic archive using pattern approach	Goal Modeling
On the identification of data related compliance problems in business processes	Others
Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective	Others
Towards a Framework for Business Process Compliance	RE Framework, Law-Compliant BP Template

Table A.6: Papers Selected from iComply

Title	**Categories**
Legal Compliant Business Processes	BP Compliance
Towards a Law Modeling Framework to Support Law-Making via BPR	BP Compliance
Making Business Processes Law Compliant	BP Compliance, Law-Compliant BP Template
Regulatory Compliance and its Impact on Software Development	Others

Table A.7: Papers Selected from RELAW

Title	**Categories**
Law, Logic and Business Processes	BP Compliance
Prioritizing Legal Requirements	Prioritization
Why Eliciting and Managing Legal Requirements Is Hard	Legal RE Extraction
Supporting Evidence-Based Compliance Evaluation for Partial Business Process Outsourcing Scenarios	BP Compliance
A Requirements-based Comparison of Privacy Taxonomies	Others
Complying with Law for RE in the Automotive Domain	RE Framework
Identifying Commitment-based Requirements to Thwart Unfair and Deceptive Practices	Legal RE Extraction

Table A.8: Papers Selected from REJ

Title	**Categories**
Addressing privacy requirements in system design: the PriS method	Others
Commitment analysis to operationalize software requirements from privacy policies	Legal RE Extraction

Table A.9: Papers Selected from RE

Title	**Categories**
Exercising Due Diligence in Legal Requirements Acquisition: A Tool-supported, Frame-Based Approach	Others
Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations	Legal RE Extraction

Table A.10: Papers Selected from CAiSE

Title	**Categories**
Exploring the Effectiveness of Normative i* Modelling: Results from a Case Study on Food Chain Traceability	Goal Modeling
Supporting the Elicitation of Requirements Compliant with Regulations	Legal RE Extraction

Table A.11: Papers Selected from Other Sources

Title	**Categories**
Analyzing Goal Semantics for Rights, Permissions, and Obligations	Goal Modeling, Legal RE Extraction
Designing Compliant Business Processes with Obligations and Permissions	BP Compliance
Analyzing Regulatory Rules for Privacy and Security Requirements	Legal RE Extraction

Appendix B

URN Legal Compliance OCL Rules

The following sections formalize in OCL the well-formedness rules of the URN legal compliance profile discussed in Section 5.3 as well as the compliance rules introduced in Section 5.5. These rules are based on the jUCMNav metamodel and use jUCMNav's predefined OCL library [80]. In this profile, stereotypes are implemented as URN metadata where the name is 'ST_Legal' and the value is the name of the stereotype (e.g., 'Obligation'). Several profile-specific helper functions are defined in Section B.3.

B.1 Well-Formedness Rules in OCL

```
-- Rule 1
context grl::IntentionalElement
inv StereotypeInLegalModelOnly:
  let s:String = self.getMetadata('ST_Legal') in
    ( s='Obligation' or s='Permission' or s='No' or s='Consequence' or
      s='Precondition' or s='XRef' or s='Exception' or 's=NoPreCondition' )
    implies
    self.isInLegalDiagram()

-- Rule 2
context grl::Actor
inv LegalStereotypesNotForActors:
  let s:String = self.getMetadata('ST_Legal') in
    ( s<>'Obligation' and s<>'Permission' and s<>'No' and s<>'Consequence'
      and s<>'Precondition' and s<>'XRef' and s<>'Exception'
      and s<>'NoPreCondition' )
```

```
-- Rule 3
context grl::Decomposition
inv ObligationNotDecomposableByNo:
  let ieSrc:grl::IntentionalElement=dest.oclAsType(IntentionalElement),
    ieDest:grl::IntentionalElement=src.oclAsType(IntentionalElement),
    s:String = ieSrc.getMetadata('ST_Legal')
  in
    (s='Obligation' and ieSrc.decompositionType=grl::DecompositionType::And)
    implies
    ieDest.getMetadata('ST_Legal') <> 'No'

-- Rule 4
context grl::Actor
inv TracesLinksBetweenActors:
  self.getLinksToForType('traces')
    -> forAll (a | a.oclIsTypeOf(grl::Actor) and a <> self)

-- Rule 5
context grl::IntentionalElement
inv TracesLinksBetweenIEs:
  self.getLinksToForType('traces')
    -> forAll (ie | ie.oclIsTypeOf(grl::IntentionalElement) and ie <> self)

-- Rule 6
context grl::Actor
inv TracesLinksFromOrgToLegalActors:
  self.getLinksToForType('traces') ->
    forAll (a | a.oclIsTypeOf(grl::Actor)
      implies
        not(self.isInLegalDiagram())
        and
        a.oclAsType(grl::Actor).isInLegalDiagram()
    )

-- Rule 7
context grl::IntentionalElement
inv TracesLinksFromOrgToLegalIEs:
  self.getLinksToForType('traces') ->
    forAll (a | a.oclIsTypeOf(grl::IntentionalElement)
      implies
        not(self.isInLegalDiagram())
        and
        a.oclAsType(grl::IntentionalElement).isInLegalDiagram()
  )

-- Rule 8
context grl::Contribution
inv ConsequenceContribFromLegalToOrg:
  let srcIE:grl::IntentionalElement = src.oclAsType(grl::IntentionalElement)
  in
    ( srcIE.isInLegalDiagram()
      and
      srcIE.getMetadata('ST_Legal') <> 'Consequence' )
```

```
    implies
    dest.oclAsType(grl::IntentionalElement).isInLegalDiagram()

-- Rule 9
context grl::Contribution
inv ConsequenceContribPositive:
  src.oclAsType(grl::IntentionalElement).getMetadata('ST_Legal') =
    'Consequence'
  implies
  self.quantitativeContribution >= 0

-- Rule 10
context grl::IntentionalElement
inv ConsequenceUnused:
  self.getMetadata('ST_Legal') = 'Consequence'
    implies
      self.linksSrc
      -> select (link | link.oclIsTypeOf(grl::Contribution))
      -> collect (link | link.oclAsType(grl::Contribution))
      -> select (c | c.dest.oclIsTypeOf(grl::IntentionalElement) and
           not(c.dest.oclAsType(grl::IntentionalElement).
               isInLegalDiagram()))
      -> size() > 0

-- Rule 11
context grl::EvaluationStrategy
inv LegalIEinitialized:
  self.evaluations.intElement
    -> forAll( ie | not(ie.isInLegalDiagram()
                  and
                  ie.name <> 'DefaultNonComp') )

-- Rule 12
context grl::IntentionalElement
inv PreconditionIsDependee:
  self.getMetadata('ST_Legal') = 'Precondition'
    implies
      self.linksDest
      -> select (link | link.oclIsTypeOf(grl::Dependency))
      -> size() > 0

-- Rule 13
context grl::IntentionalElement
inv PreconditionSatisfactionValue:
  self.getMetadata('ST_Legal') = 'Precondition'
  implies
  (getNumEval() = 100 or getNumEval() = 0)

-- Rule 14
context grl::IntentionalElement
inv XRefHasURNLink:
  let s:String = getMetadata('ST_Legal') in
    (s = 'XRef')
```

```
    implies
    self.getLinksToForType('external')
      -> size() > 0

-- The following four rules apply to the consequence model included in the
-- URN model combining the legal and organization models

-- Rule 15
context grl::IntentionalElement
inv ConsequenceWithMinus100Contrib:
  self.getMetadata('ST_Legal') = 'Consequence'
    implies
      self.linksDest
      -> select (link | link.oclIsTypeOf(grl::Contribution))
      -> collect (link | link.oclAsType(grl::Contribution))
      -> one (c | c.quantitativeContribution = -100
          and c.src.oclIsTypeOf(grl::IntentionalElement)
          and c.src.oclAsType(grl::IntentionalElement).name =
              'DefaultNonComp' )

-- Rule 16
context grl::IntentionalElement
inv ConsequenceDependOnDefaultMaxEval:
  self.getMetadata('ST_Legal') = 'Consequence'
    implies
      self.linksDest
      -> select (link | link.oclIsTypeOf(grl::Dependency))
      -> collect (link | link.oclAsType(grl::Dependency))
      -> one (d | d.src.oclIsTypeOf(grl::IntentionalElement)
          and d.src.oclAsType(grl::IntentionalElement).name =
              'DefaultMaxEval' )

-- Rule 17
context grl::IntentionalElement
inv DefaultNonCompSetTo100:
  self.name = 'DefaultNonComp' implies
    type=IntentionalElementType::Ressource and isInLegalDiagram() and
      (getNumEval() = 100 or getNumEval() = -1000)


-- Rule 18
context grl::IntentionalElement
inv DefaultMaxEvalSetToZero:
  self.name = 'DefaultMaxEval' implies
    type=IntentionalElementType::Ressource and isInLegalDiagram() and
      (getNumEval() = 0 or getNumEval() = -1000)
```

B.2 Compliance Rules in OCL

These OCL rules have access to the satisfaction values of intentional elements (after having run a GRL strategy) through the getNumEval() predefined function. This function returns −1000 if there was an evaluation error on that intentional element.

```
-- Rule 19
context grl::IntentionalElement
inv ObligationFullySatisfied:
  self.getMetadata('ST_Legal') = 'Obligation' implies
    (getNumEval() = 100 or getNumEval() = -1000)

-- Rule 20
context grl::IntentionalElement
inv PermissionFullySatisfied:
  self.getMetadata('ST_Legal') = 'Permission' implies
    ( (self.linksDest
      -> select (link | link.oclIsTypeOf(grl::Decomposition))
      -> collect (link | link.oclAsType(grl::Decomposition))
      -> exists (d | d.src.oclIsTypeOf(grl::IntentionalElement)
                     and d.src.oclAsType(grl::IntentionalElement).
                         getMetadata('ST_Legal') <> 'No')
    ) implies
      (self.getNumEval() = 100 or self.getNumEval() = -1000) )

-- Rule 21
context grl::IntentionalElement
inv NonComplianceOnTracesIEs:
  self.getLinksToForType('traces')
    -> forAll (ie | ie.oclIsTypeOf(grl::IntentionalElement)
      implies
      self.getNumEval() <= ie.getNumEval() )

-- Rule 22
context grl::Actor
inv NonComplianceOnTracesActors:
  self.getLinksToForType('traces')
    -> forAll (a | a.oclIsTypeOf(grl::Actor)
      implies
      self.getNumEval() <= a.getNumEval() )

-- Rule 23
context grl::IntentionalElement
inv NonComplianceOnPrecondition:
  self.getMetadata('ST_Legal') = 'Precondition' implies
  ( (self.linksDest
      -> select (link | link.oclIsTypeOf(grl::Dependency))
      -> collect (link | link.oclAsType(grl::Dependency))
      -> forAll (ie | ie.oclIsTypeOf(grl::IntentionalElement)
      implies
      (self.getNumEval() = ie.getNumEval()) ) )
```

B.3 GRL Legal Profile Helper Functions

```
package urncore
context Actor
def: isInLegalDiagram():Boolean =
  -- Checks whether the actor is present in a legal diagram
  self.contRefs.diagram
    -> select(d|d.oclIsTypeOf(grl::GRLGraph))
    -> collect(d|d.oclAsType(grl::GRLGraph))
    -> select(d|d.getMetadata('ST_Legal')='Legal')
    -> size() > 0

context IntentionalElement
def: isInLegalDiagram():Boolean =
  -- Checks whether the intentional element is present in a legal diagram
  self.refs.diagram
    -> select(d|d.oclIsTypeOf(grl::GRLGraph))
    -> collect(d|d.oclAsType(grl::GRLGraph))
    -> select(d|d.getMetadata('ST_Legal')='Legal')
    -> size() > 0

-- For accessing evaluation values
context URNmodelElement
def: getNumEval():Integer =
    let e:String = self.getMetadata('_numEval') in
      if (e <> '')
      then e.toInteger()
      else -1000  -- Error code.
      endif

def: getQualEval():String =
    self.getMetadata('_qualEval')
endpackage
```

Appendix C

Parts of PHIPA Hohfeldian and GRL Models

This appendix presents some of the PHIPA statements we modeled using the LEGAL-URN framework for Chapter 4, the case study in Chapters 5 and 6.

C.1 Article 10 - Information Practices

Information practices

10.(1) An HIC that has custody or control of PHI *shall* have in place information practices that comply with the requirements of this Act and its regulations. → Duty-Claim Statement → Obligation Goal.

Table C.1 summarizes the statement's parts.

Duty to follow practices

(2) An HIC *shall* comply with its information practices. → Duty-Claim Statement → Obligation Goal.

Table C.2 summarizes the statement's parts.

Table C.1: PHIPA - Article 10 (1)

Section	Information practices
Actor	An HIC
Modal Verb	Shall
Clause	Have in place information practices that comply with the requirements of this Act and its regulations.
Precondition	Has custody or control of PHI

Table C.2: PHIPA - Article 10 (2)

Section	Information practices
Actor	An HIC
Modal Verb	Shall
Clause	Comply with information practices.
Precondition	-

Use of electronic means

(3) An HIC that uses electronic means to collect, use, modify, disclose, retain or dispose of PHI *shall* comply with the prescribed requirements, if any. → Duty-Claim Statement → Obligation Goal.

Table C.3 summarizes the statement's parts.

Table C.3: PHIPA - Article 10 (3)

Section	Information practices
Actor	An HIC
Modal Verb	Shall
Clause	Comply with the prescribed requirements, if any.
Precondition	That uses electronic means to collect, [...] of PHI

Providers to custodians

(4) A person who provides goods or services for the purpose of enabling and HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI *shall* comply with the prescribed requirements, if any. → Duty-Claim Statement → Obligation Goal.

Table C.4 summarizes the statement's parts and Figure C.1 shows Articles 10(1) - 10(4) modeled in Legal GRL.

Table C.4: PHIPA - Article 10 (4)

Section	Information practices
Actor	A person
Modal Verb	Shall
Clause	Comply with the prescribed requirements, if any.
Precondition	Who provides goods or services for the purpose of enabling and HIC to use [...] of PHI

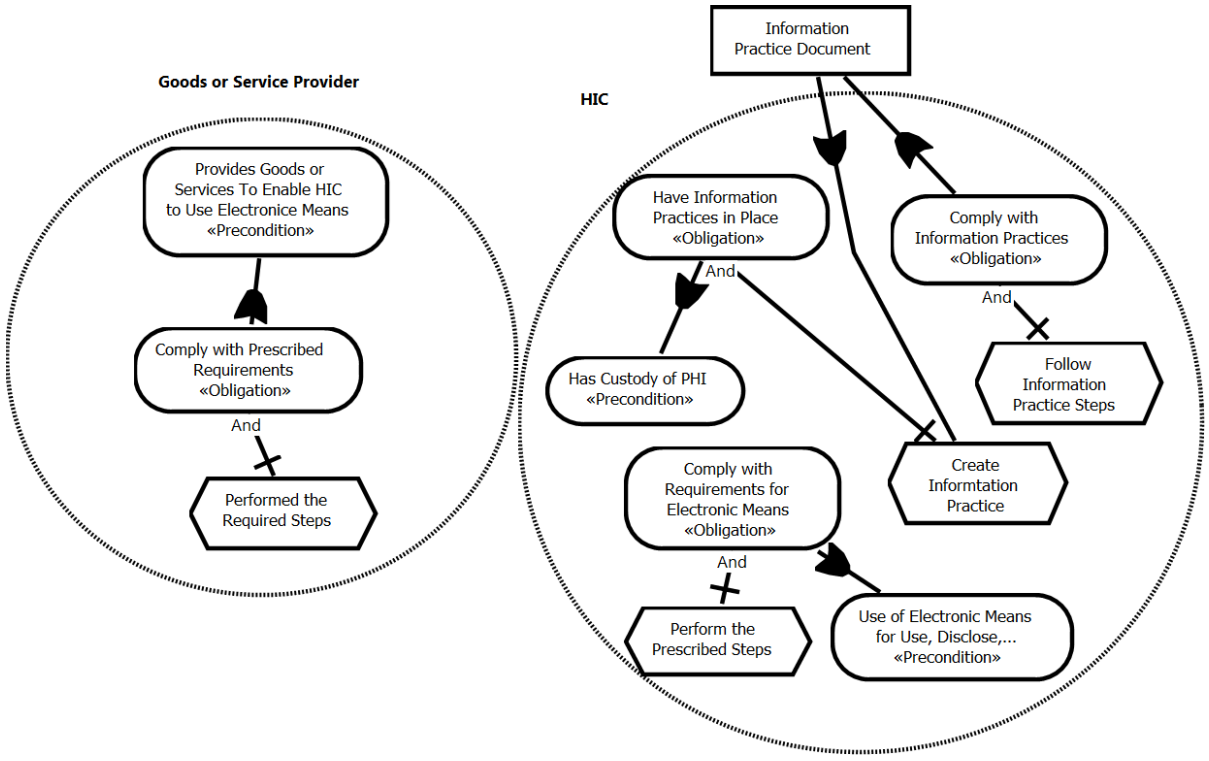

Figure C.1: PHIPA - Article 10

C.2 Article 11 - Accuracy

Accuracy

11.(1) An HIC that uses PHI about an individual *shall* take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes for which it uses the information. → Duty-Claim Statement → Obligation Goal. (Refer to: Table C.5 and Figure C.2)

Table C.5: PHIPA - Article 11 (1)

Section	Accuracy
Actor	An HIC
Modal Verb	Shall
Clause	Take reasonable steps to ensure that the information [...]
Precondition	-

Same, disclosure

(2) An HIC that discloses PHI about an individual *shall*,

(a) take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes of the disclosure that are known to the custodian at the time of the disclosure; or → Duty-Claim Statement → Obligation Goal.

(b) clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information. → Duty-Claim Statement → Obligation Goal.

Table C.6 summarizes the statement's parts and Figure C.2 shows Articles 11(1) and 11(2) modeled in Legal GRL.

Table C.6: PHIPA - Article 11 (2)

Section	Accuracy
Actor	An HIC
Modal Verb	Shall
Clause 1	Take reasonable steps to ensure that the information is as accurate, complete and up-to-date [...]
Clause 2	Clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, [...]
Precondition	That discloses PHI about an individual

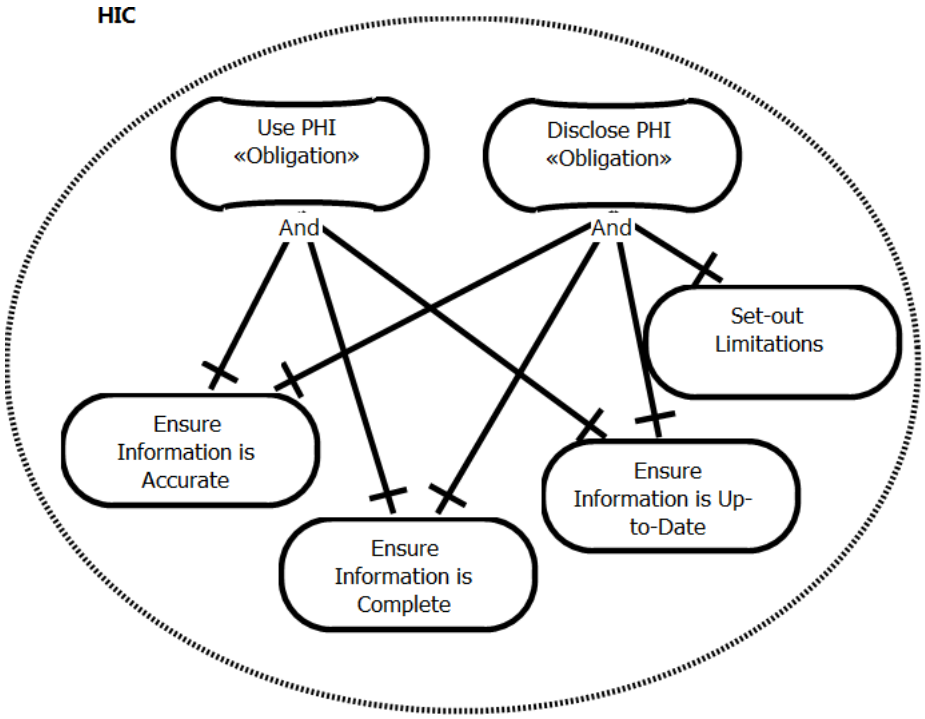

Figure C.2: PHIPA - Article 11

C.3 Article 12 - Security

Security

12. (1) An HIC *shall* take steps that are reasonable in the circumstances to ensure that PHI in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. Two → Duty-Claim Statements

→ Obligation Goals. See Table C.7 and Figure C.3.

Table C.7: PHIPA-Article 12 (1)

Section	Security
Actor	An HIC
Modal Verb	Shall
Clause 1	Take steps [...] is protected against theft, loss and unauthorized use or disclosure
Clause 2	To ensure that the records [...] are protected against unauthorized copying, modification or disposal
Precondition	-

Notice of loss, etc.

(2) Subject to subsection (3) and subject to the exceptions and additional requirements, if any, that are prescribed, an HIC that has custody or control of PHI about an individual *shall* notify the individual at the first reasonable opportunity *if* the information is stolen, lost, or accessed by unauthorized persons. → Duty-Claim Statement → Obligation Goal (based on a privacy breach condition).See Table C.8 and Figure C.3.

Table C.8: PHIPA - Article 12 (2)

Section	Security
Actor	An HIC
Precondition	That has custody or control of PHI about an individual
Modal Verb	Shall
Clause 1	Notify the individual at the first reasonable opportunity
Clause 2	Clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, [...]
Precondition 2	If the information is stolen, lost, or accessed by unauthorized persons

Exception

(3) *If* the HIC is a researcher who has received the PHI from another health information custodian under subsection 44 (1), the researcher *shall not* notify the individual that

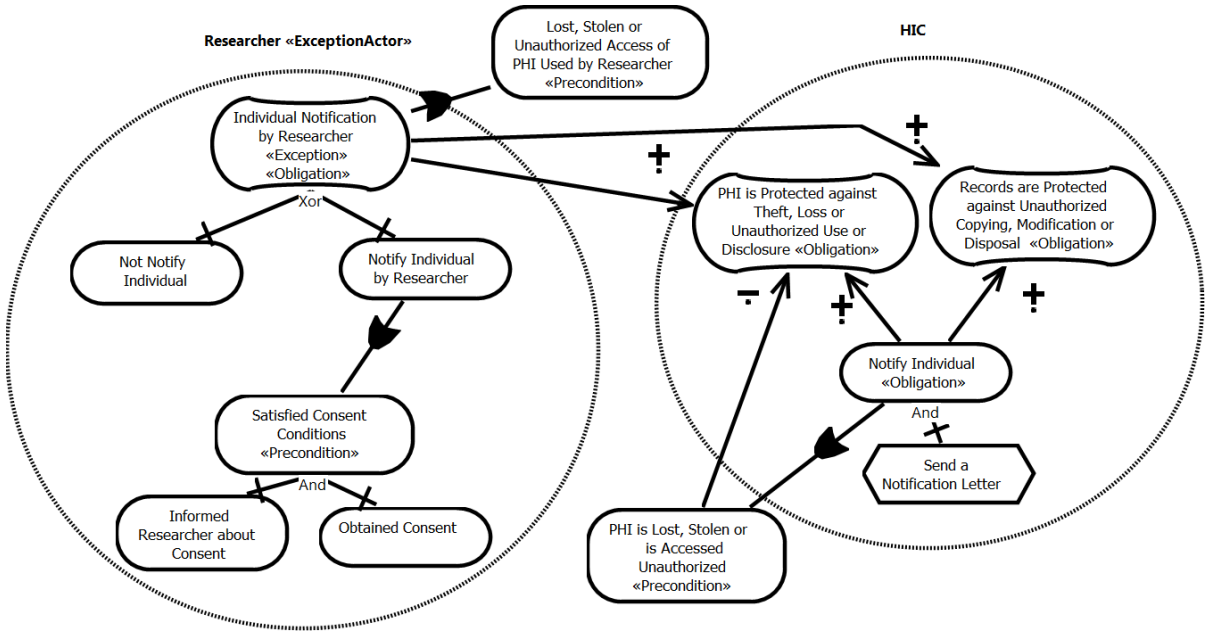

Figure C.3: PHIPA - Article 12

the information is stolen, lost or accessed by unauthorized persons *unless* the HIC under that subsection first obtains the individual's consent to having the researcher contact the individual and informs the researcher that the individual has given the consent. → Duty-Claim and Privilege-NoClaim Statements → Obligation and Permission Goals. See Table C.9 and Figure C.3.

Table C.9: PHIPA-Article 12 (3)

Section	Security
Actor	The researcher
Modal Verb	Shall
Clause	Not notify the individual that the information is [...]
Precondition	HIC is a researcher [...]
Precondition	HIC obtain individual consent for contacting and informed researcher[...]
Exception	Notify

C.4 Article 18 - Elements of Consent

Elements of consent

18.(1) If this Act or any other Act requires the consent of an individual for the collection, use or disclosure of PHI by an HIC, the consent, (Table C.10 and Figure C.4)

(a) *must* be a consent of the individual;

(b) *must* be knowledgeable;

(c) *must* relate to the information; and

(d) *must not* be obtained through deception or coercion.

→ Duty-Claim Statement → Obligation Goal.

Table C.10: PHIPA - Article 18 (1)

Section	Elements of Consent
Actor	-
Modal Verb	Must
Clause	(a) to (d)
Precondition	If this Act or any other Act requires the consent of an individual for [...]

Implied consent

(2) Subject to subsection (3), a consent to the collection, use or disclosure of personal health information about an individual *may be* express or implied. → Privilege-NoClaim Statement → Permission Goal. See Table C.11 and Figure C.4.

Table C.11: PHIPA - Article 18 (2)

Section	Elements of Consent
Actor	-
Modal Verb	May
Clause	Be express or implied
Precondition	-

Exception

(3) A consent to the disclosure of PHI about an individual *must* be express, and not implied, *if*,

(a) an HIC makes the disclosure to a person that is not an HIC; or

(b) an HIC makes the disclosure to another HIC and the disclosure is not for the purposes of providing health care or assisting in providing health care.

→ Duty-Claim Statement → Obligation Goal. See Table C.12 and Figure C.4.

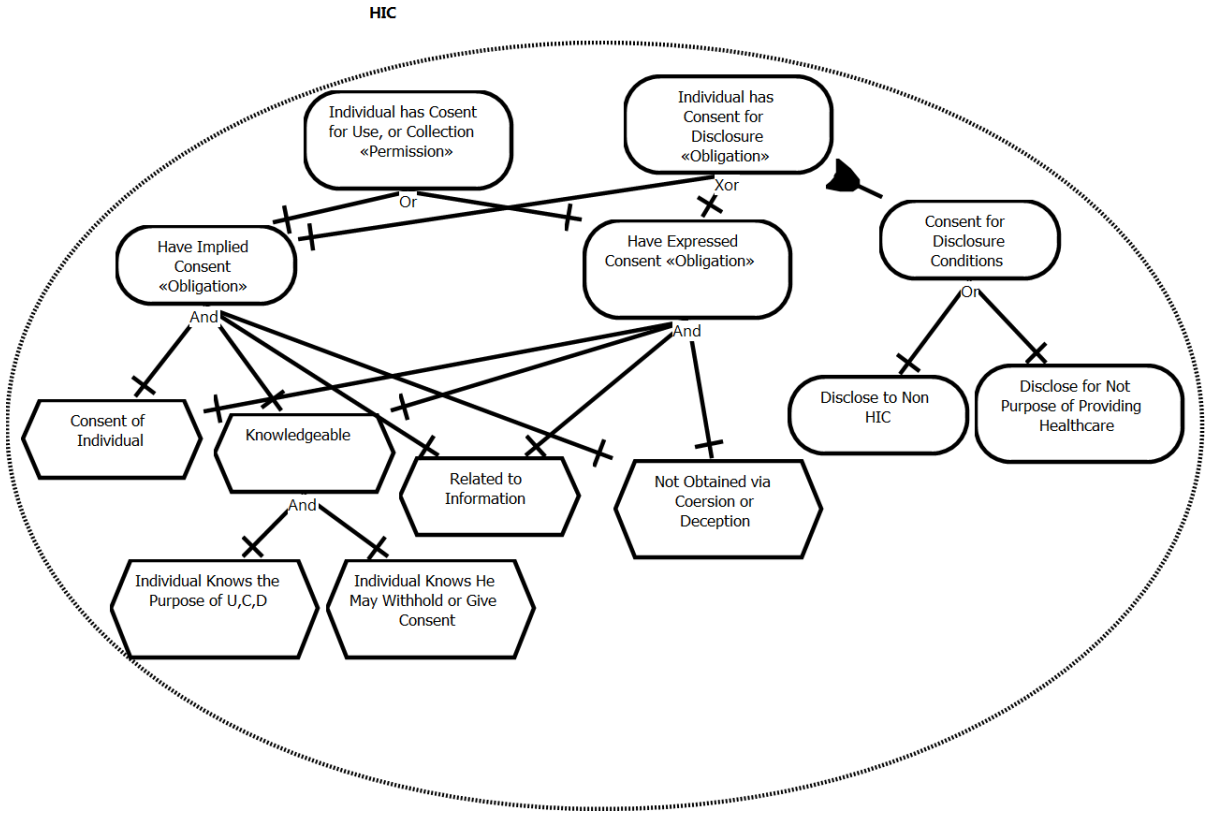

Figure C.4: PHIPA - Article 18(3)

Statement: Consent to the disclosure of PHI *must* be expressed.

Table C.12: PHIPA-Article 18 (3)

Section	Elements of Consent
Actor	-
Modal Verb	Must
Clause	be express, and not implied
Precondition 1	An HIC makes the disclosure to a person that is not an HIC
Precondition 2	An HIC makes the disclosure to another HIC and the disclosure is not for the purposes of [...]

C.5 Article 36 - Indirect Collection

Indirect Collection

36.(1) An HIC *may* collect PHI about an individual indirectly if, → Privilege-NoClaim Statement → Permission Goal. See Table C.13 and Figure C.5.

Table C.13: PHIPA - Article 36 (1)

Section	Indirect Collection
Actor	An HIC
Modal Verb	May
Clause	Collect PHI about an individual indirectly
Precondition	(a) - (h)

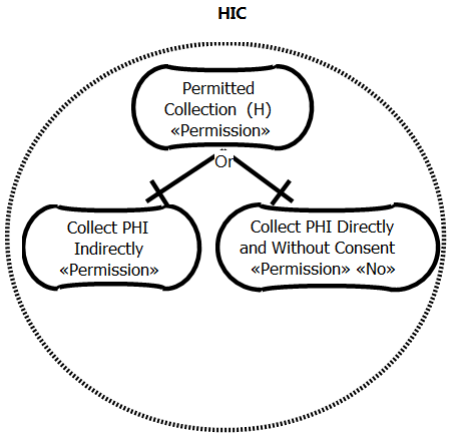

Figure C.5: PHIPA - Article 36 - Permitted Collection

(a) the individual consents to the collection being made indirectly; (Figure C.6)

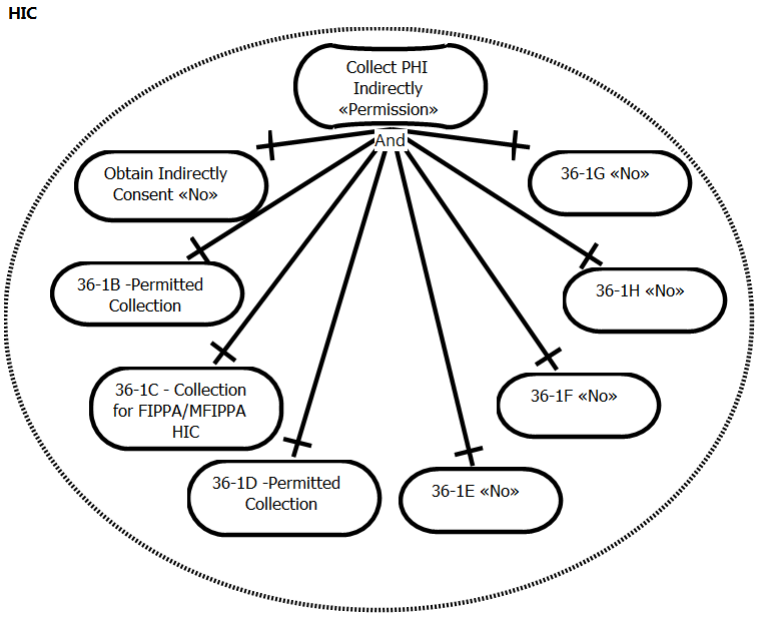

Figure C.6: PHIPA - Article 36 - 1 - Indirect Collection

(b) the information to be collected is reasonably necessary for providing health care or assisting in providing health care to the individual and it is not reasonably possible to collect, directly from the individual, (Figure C.7)

(i) PHI that can reasonably be relied on as accurate and complete, or

(ii) PHI in a timely manner;

(c) the custodian is an institution within the meaning of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act, or is acting as part of such an institution, and the custodian is collecting the information for a purpose related to, → Refer to FIPPA or MFIPPA, and see Figure C.8.

(i) investigating a breach of an agreement or a contravention or an alleged contravention of the laws of Ontario or Canada,

(ii) the conduct of a proceeding or a possible proceeding, or

(iii) the statutory function of the custodian;

(d) the custodian collects the information from a person who is not an HIC for the purpose of carrying out research conducted in accordance with subsection 37 (3) or

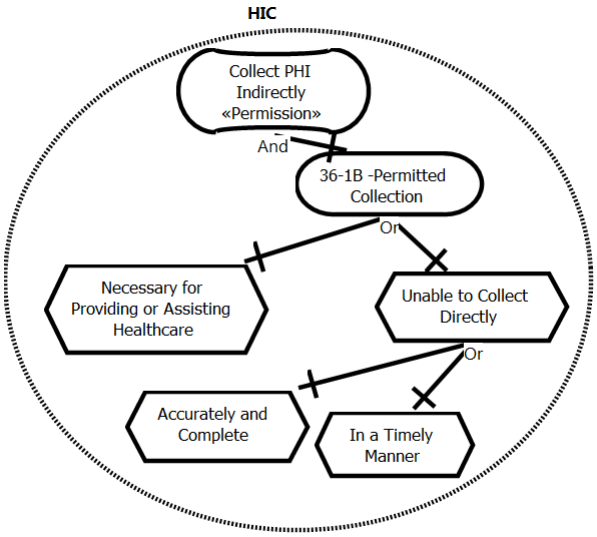

Figure C.7: PHIPA - Article 36 - 1b

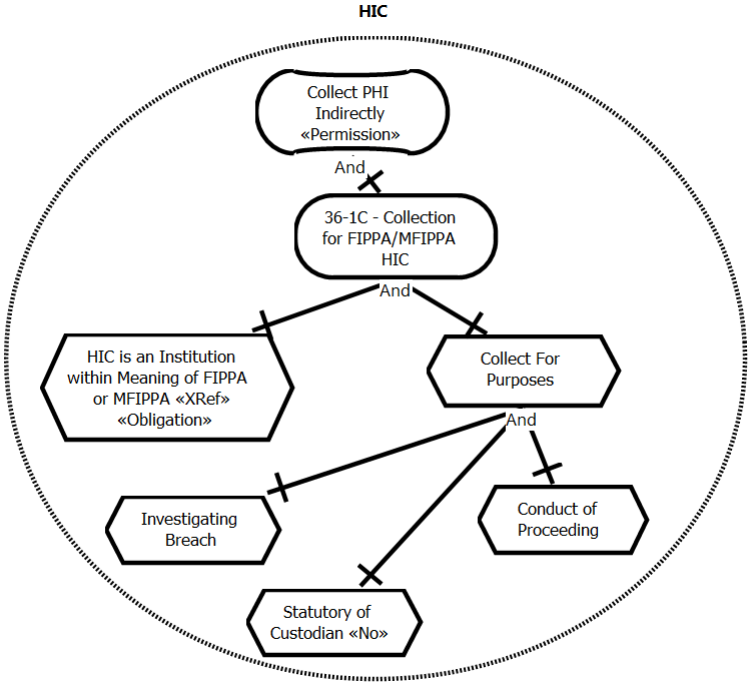

Figure C.8: PHIPA - Article 36 - 1c

research that an REB has approved under section 44 or that meets the criteria set out in clauses 44 (10) (a) to (c), except if the person is prohibited by law from disclosing the information to the custodian; → See subsections 37(3) and 44(10), and Figure C.9.

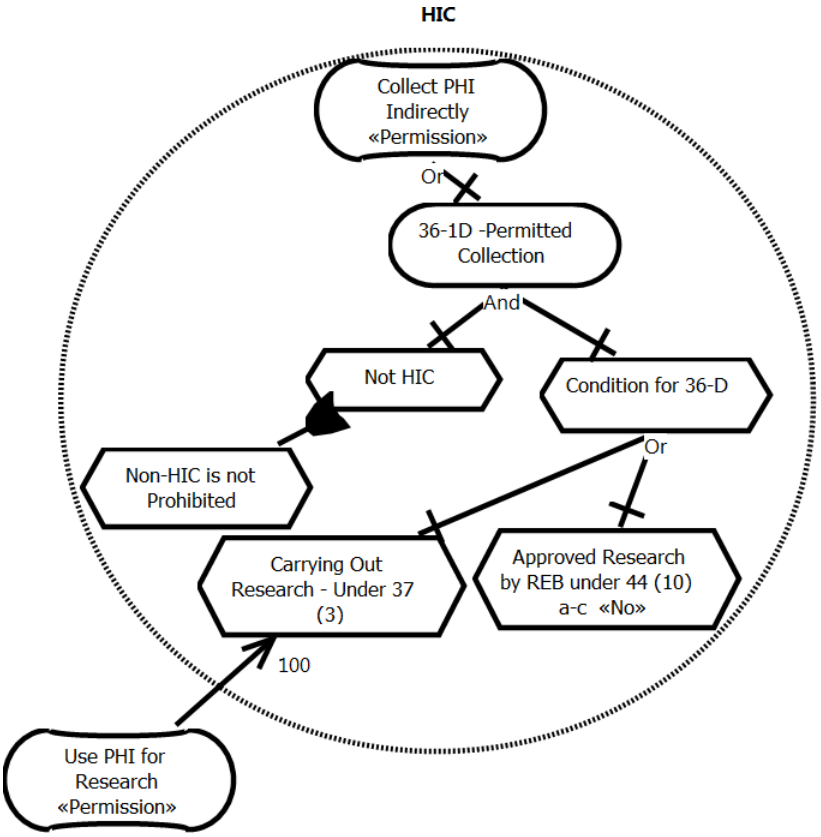

Figure C.9: PHIPA - Article 36-1d

(e) the custodian is a prescribed entity mentioned in subsection 45 (1) and the custodian is collecting personal health information from a person who is not a health information custodian for the purpose of that subsection; (Figure C.10)

(f) the Commissioner authorizes that the collection be made in a manner other than directly from the individual; (Figure C.11)

(g) the custodian collects the information from a person who is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to disclose it to the custodian; or (Figure C.12)

(h) subject to the requirements and restrictions, if any, that are prescribed, the health information custodian is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to collect the information indirectly. (Figure C.13)

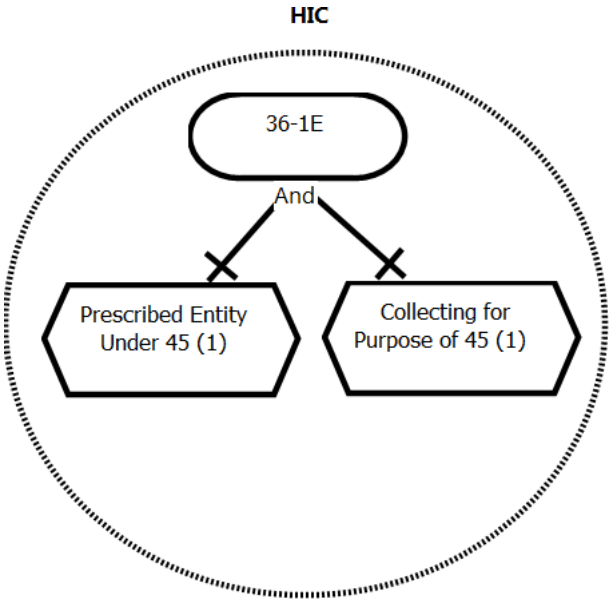

Figure C.10: PHIPA - Article 36-1e

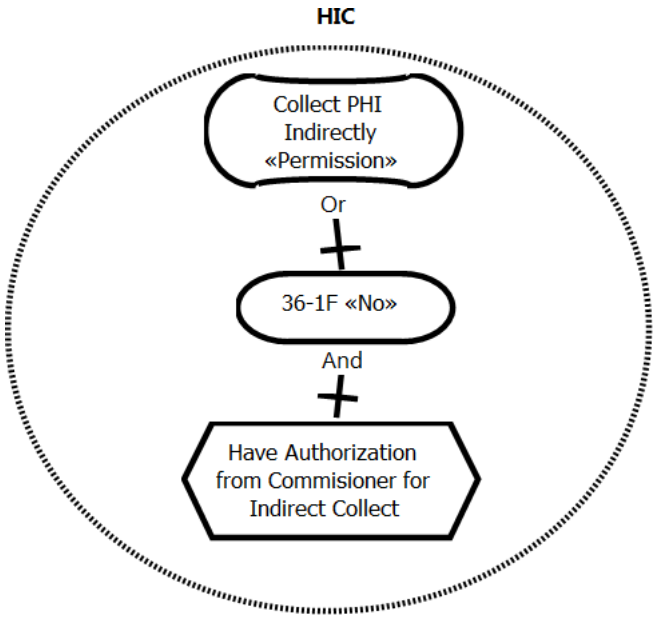

Figure C.11: PHIPA - Article 36-1f

Direct collection without consent

(2) An HIC *may* collect PHI about an individual directly from the individual, even if the individual is incapable of consenting, if the collection is reasonably necessary for

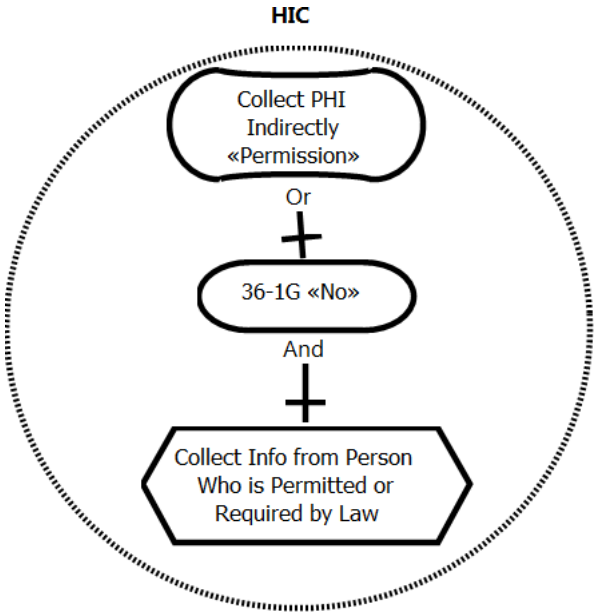

Figure C.12: PHIPA - Article 36-1g

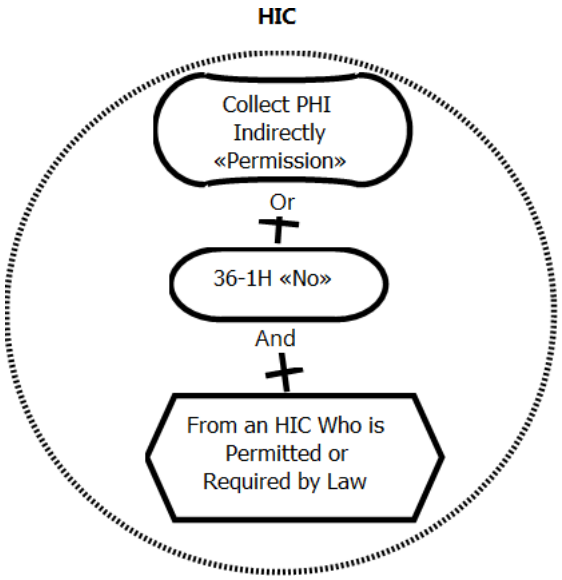

Figure C.13: PHIPA - Article 36-1h

the provision of health care and it is not reasonably possible to obtain consent in a timely manner. → Privilege-NoClaim Statement → Permission Goal. See Table C.14 and Figure C.14.

Table C.14: PHIPA - Article 36 (2)

Section	Indirect Collection
Actor	An HIC
Modal Verb	May
Clause	Collect PHI about an individual directly [...] even if the individual is incapable of consenting
Precondition	If the collection is reasonably necessary for the provision of health care and it is not reasonably possible to obtain consent in a timely manner.

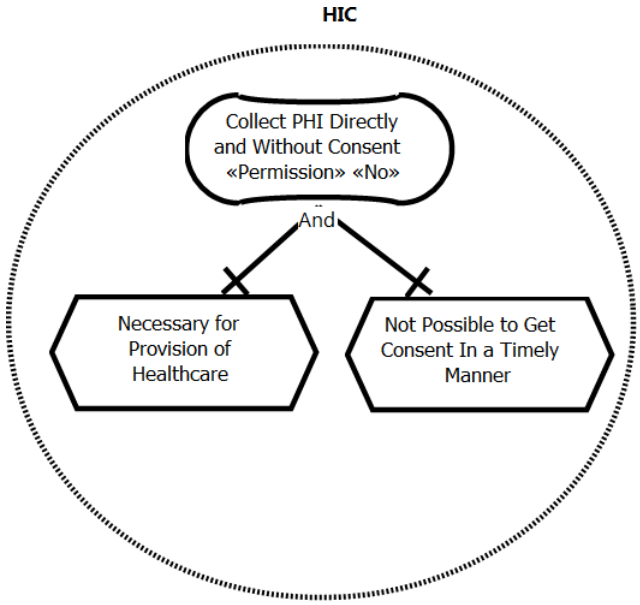

Figure C.14: PHIPA - Article 36-2

C.6 Article 37 - Permitted Use

37.(1) An HIC *may* use PHI about an individual, → Privilege-NoClaim Statement → Permission Goal. See Table C.15 and Figure C.15).

Table C.15: PHIPA - Article 37 (1)

Section	Permitted Use
Actor	An HIC
Modal Verb	May
Clause	Use PHI about an individual for (a) - (k)
Precondition	-

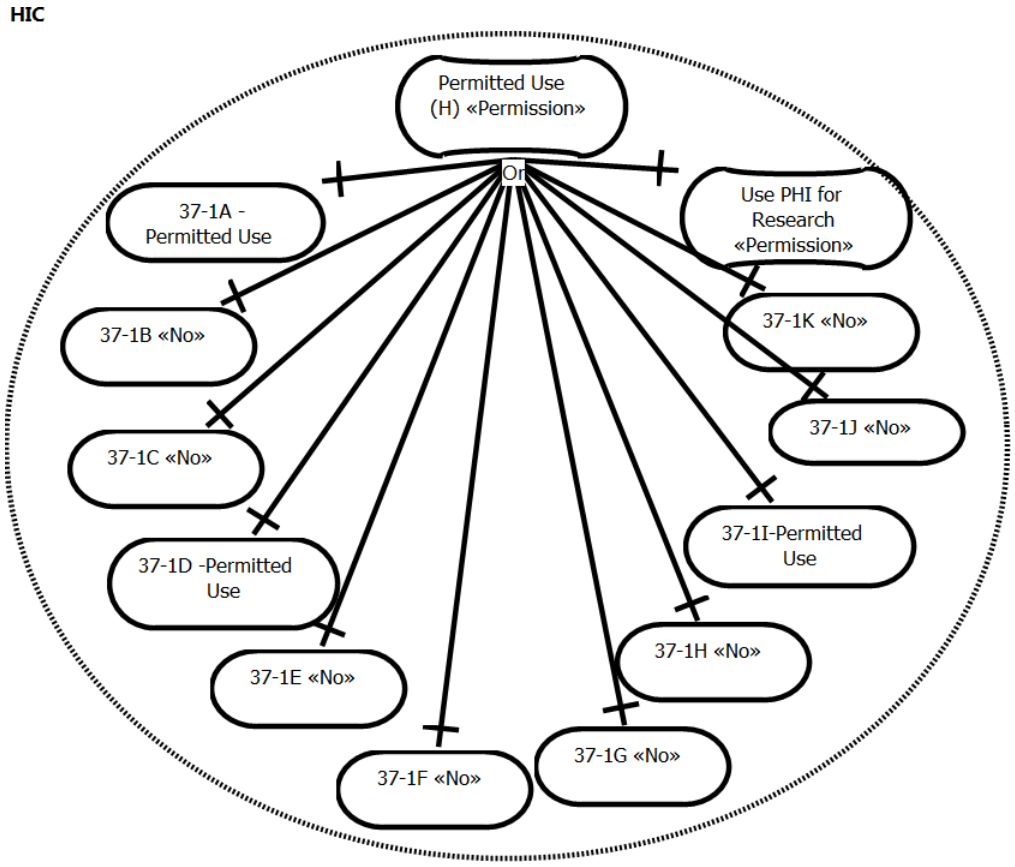

Figure C.15: PHIPA - Article 37 (1) (General)

(a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent of the individual or under clause 36 (1) (b) and the individual expressly instructs otherwise; (Figure C.16)

(b) for a purpose for which this Act, another Act or an Act of Canada permits or requires a person to disclose it to the custodian; (Figure C.17)

(c) for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them;(Figure C.18)

(d) for the purpose of risk management, error management or for the purpose of

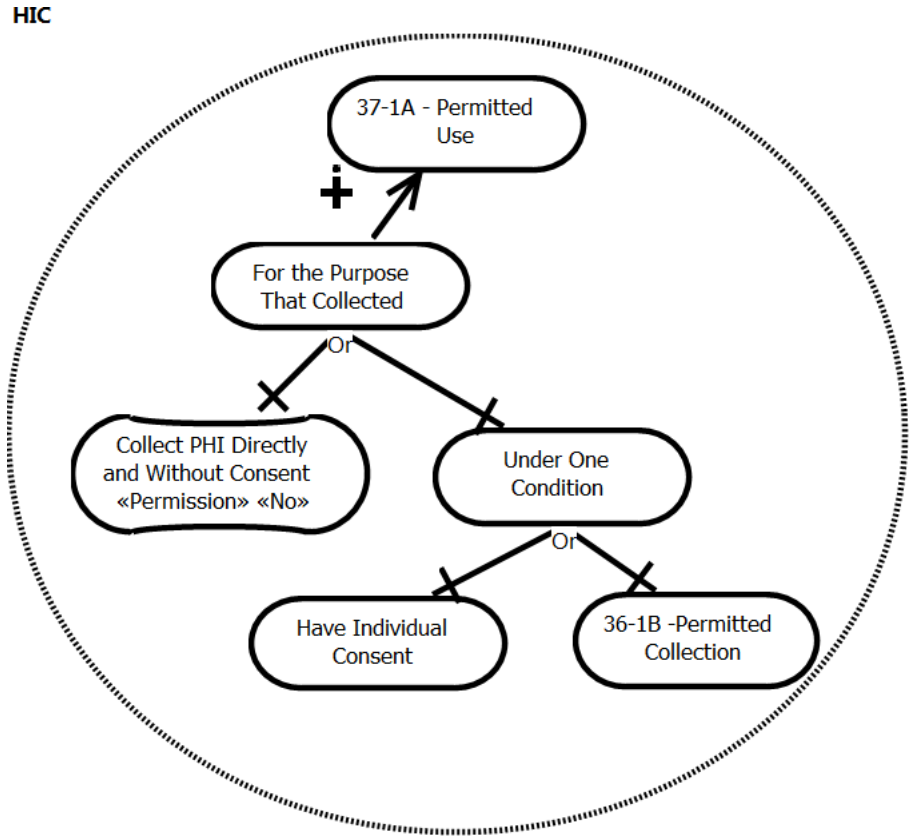

Figure C.16: PHIPA - Article 37-1a

activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian; (Figure C.19)

(e) for educating agents to provide health care; (Figure C.20)

(f) in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual; (Table C.15 and Figure C.21)

(g) for the purpose of seeking the individual's consent, or the consent of the individual's substitute decision-maker, when the personal health information used by the custodian for this purpose is limited to the name and contact information of the individual and the name and contact information of the substitute decision-maker, where applicable;

(h) for the purpose of a proceeding or contemplated proceeding in which the custodian

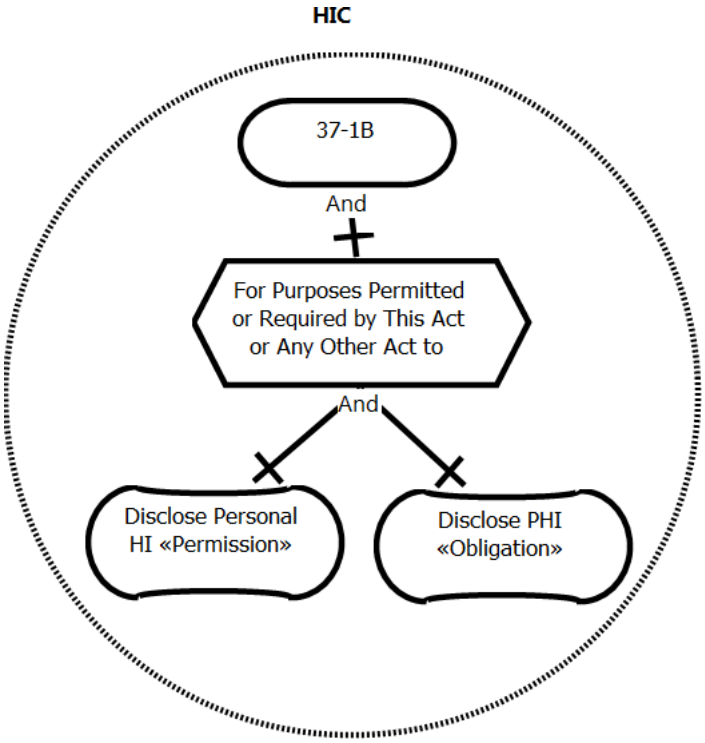

Figure C.17: PHIPA - Article 37-1b

or the agent or former agent of the custodian is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding;

(i) for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services; (Figure C.22)

(j) for research conducted by the custodian, subject to subsection (3), unless another clause of this subsection applies; or (Table C.15 and Figure C.23)

(k) subject to the requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada. Agents

(2) If subsection (1) authorizes an HIC to use PHI for a purpose, the custodian *may* provide the information to an agent of the custodian who may use it for that purpose on

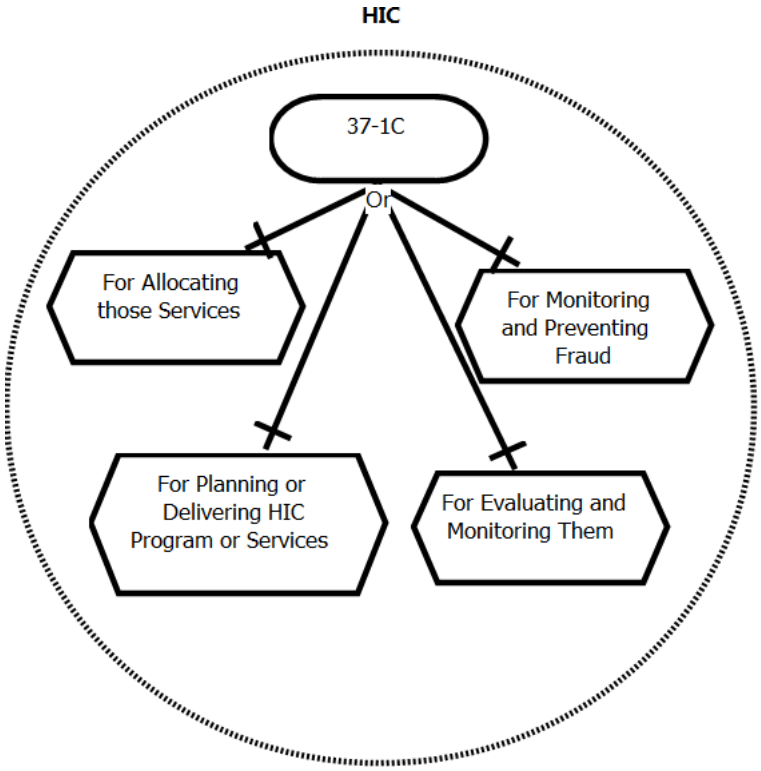

Figure C.18: PHIPA - Article 37-1c

behalf of the custodian. → Privilege-NoClaim Statement → Permission Goal.

Table C.16: PHIPA - Article 37 (2)

Section	Permitted Use
Actor	An HIC
Modal Verb	May
Clause	Provide the information to an agent of the custodian who may use it for that purpose on behalf of the custodian
Precondition	If subsection (1) authorizes an HIC to use PHI for a purpose

Research

(3) Under clause (1) (j), an HIC *may* use PHI about an individual only if the custodian prepares a research plan and has an REB approve it and for that purpose subsections 44 (2) to (4) and clauses 44 (6) (a) to (f) apply to the use as if it were a disclosure. →

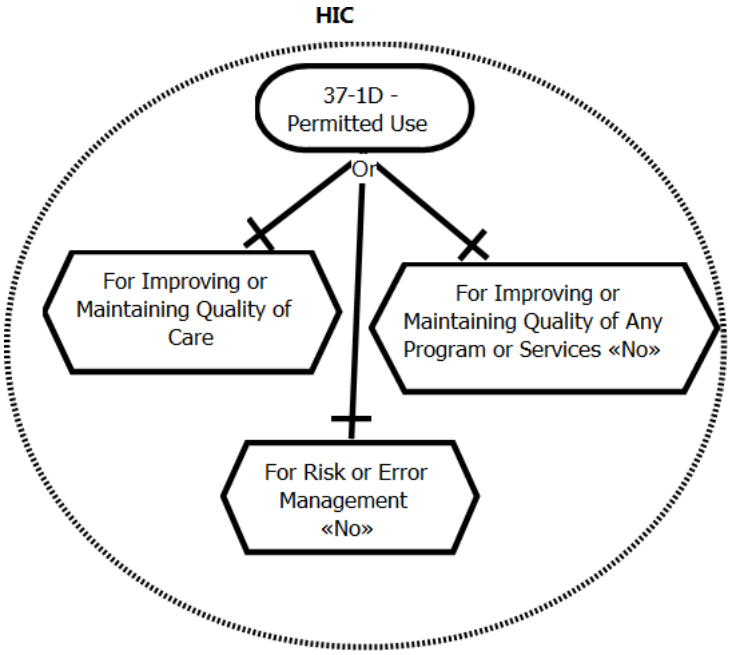

Figure C.19: PHIPA - Article 37-1d

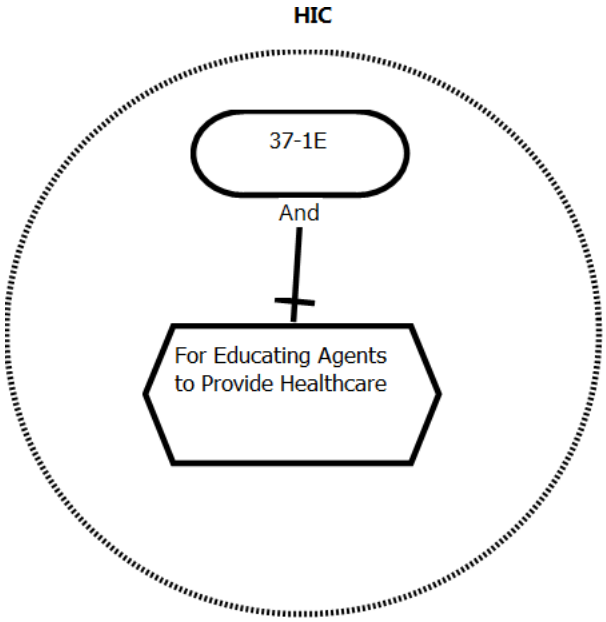

Figure C.20: PHIPA - Article 37-1e

Privilege-NoClaim Statement → Permission Goal. See Table C.17 and Figure C.24.

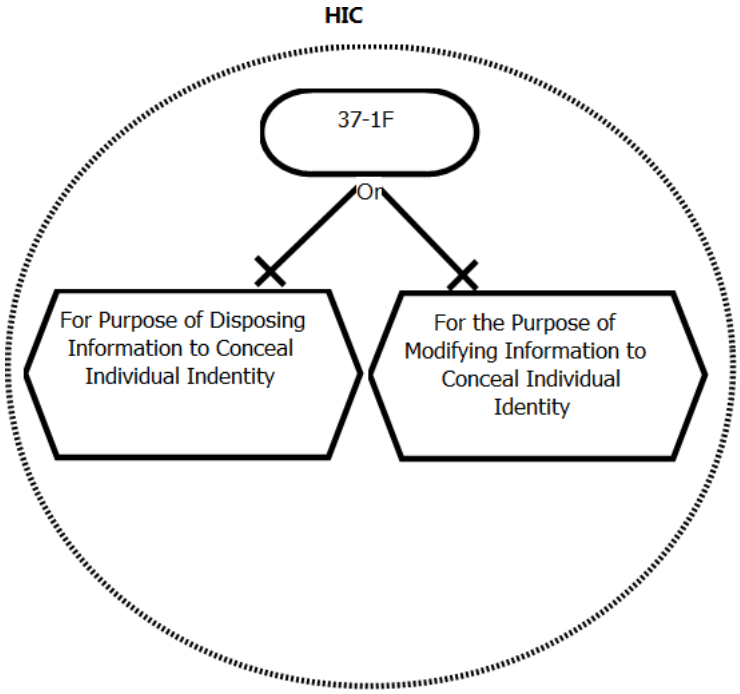

Figure C.21: PHIPA - Article 37-1F

Table C.17: PHIPA - Article 37 (3)

Section	Permitted Use
Actor	An HIC
Modal Verb	May
Clause	Use PHI about an individual
Precondition 1	Only if the custodian prepares a research plan and has a research ethics board approve it and
Precondition 1	For that purpose subsections 44 (2) to (4) and clauses 44 (6) (a) to (f) apply to the use as if it were a disclosure

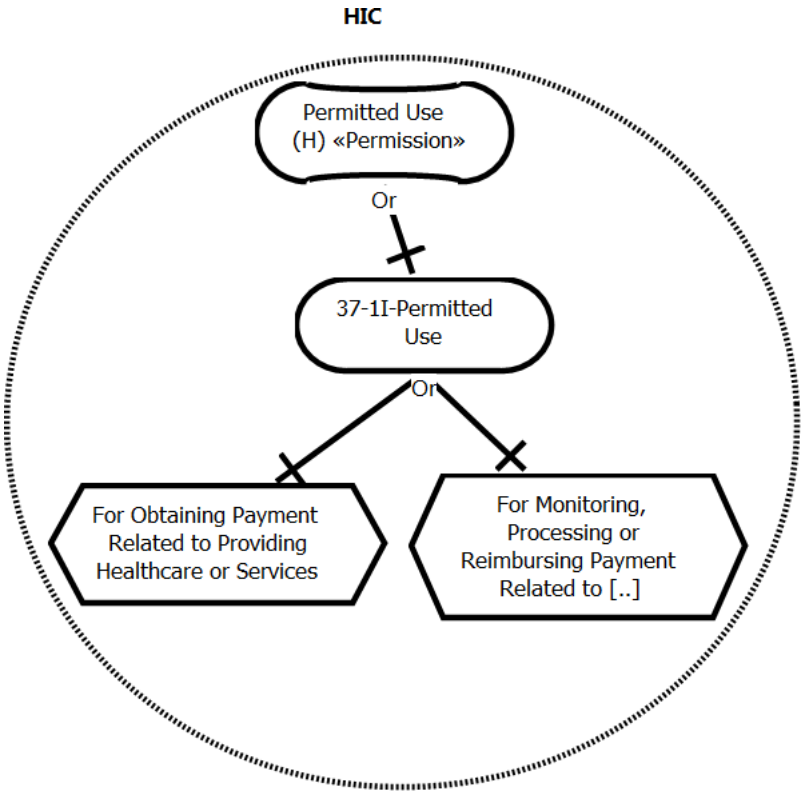

Figure C.22: PHIPA - Article 37-1i

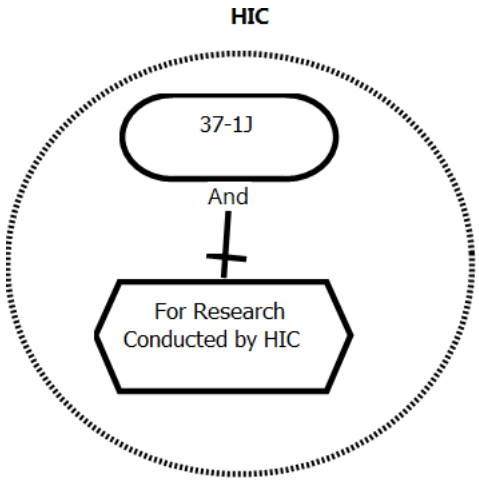

Figure C.23: PHIPA - Article 37-1j

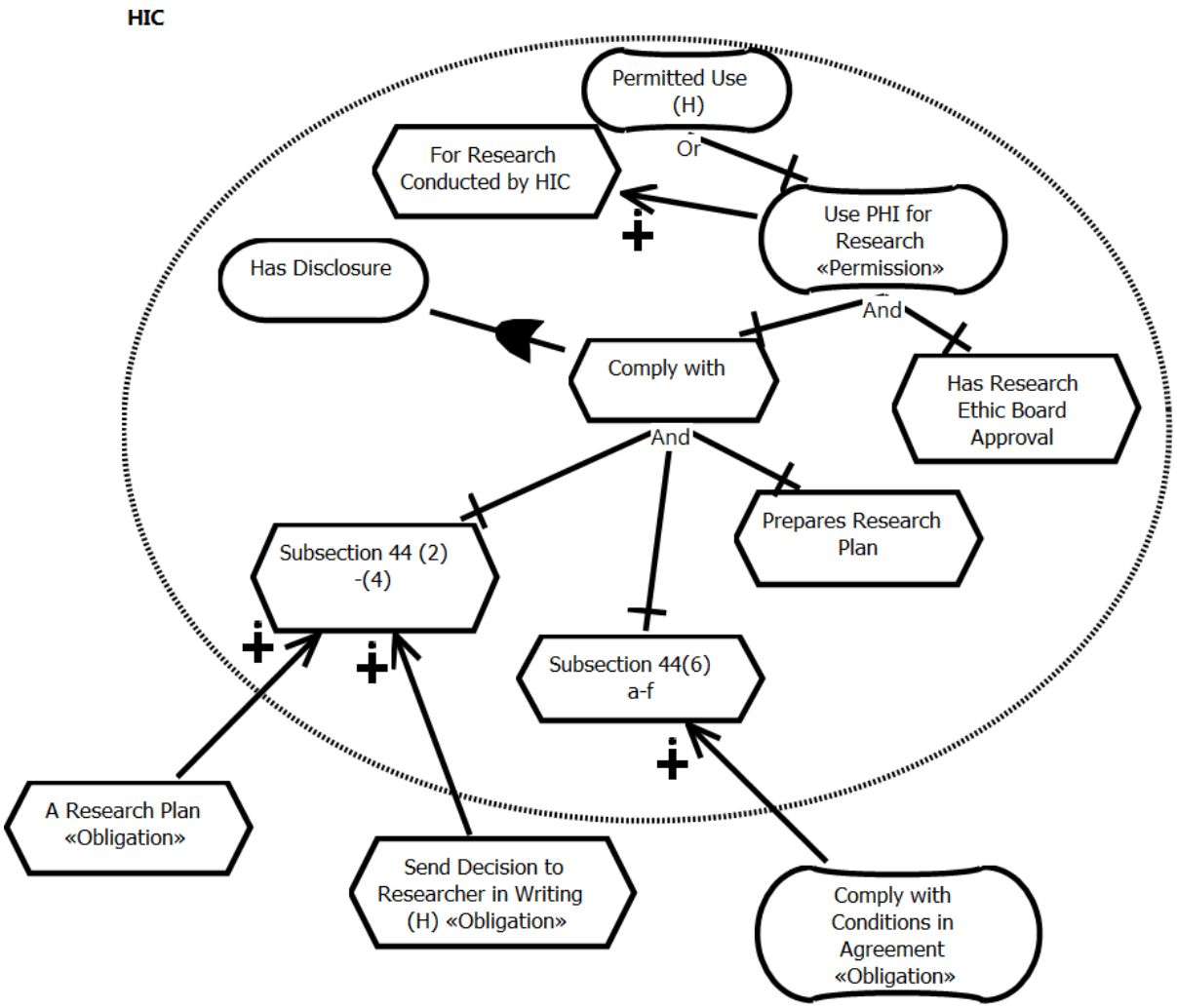

Figure C.24: PHIPA - Article 37-3

C.7 Article 38 - Disclosures Related to Providing Health Care

38.(1) An HIC *may* disclose PHI about an individual, → Privilege-NoClaim Statement → Permission Goal. See Table C.18 and Figure C.25.

Table C.18: PHIPA-Article 38 (1)

Section	Disclosures Related to Providing Health Care
Actor	An HIC
Modal Verb	May
Clause 1	Disclose PHI about an individual to an HIC described in [...]
Precondition 1	If the disclosure is reasonably necessary for [...] and it is not reasonably possible to obtain the individual's consent in a timely manner,
Exception 1	But not if the individual has expressly instructed the custodian not to make the disclosure;
Clause 2	Disclose PHI about an individual in order for the Minister, another HIC or a local health integration network to determine or [...]
Clause 3	Disclose PHI about an individual for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual
Precondition 3	If the individual is injured, incapacitated or ill and unable to give consent personally.

(a) to an HIC described in paragraph 1, 2, 3 or 4 of the definition of "HIC" in subsection 3 (1), if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner, but not if the individual has expressly instructed the custodian not to make the disclosure; (Figure C.26)

(b) in order for the Minister, another HIC or a local health integration network to determine or provide funding or payment to the custodian for the provision of health care; or (Figure C.27)

(c) for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual, if the individual is injured, incapacitated or ill and unable to give consent personally. (Figure C.28)

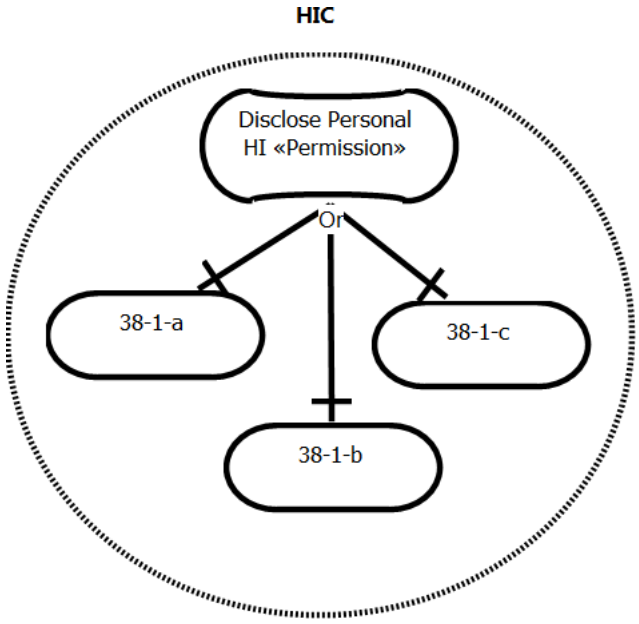

Figure C.25: PHIPA - Article 38 -1

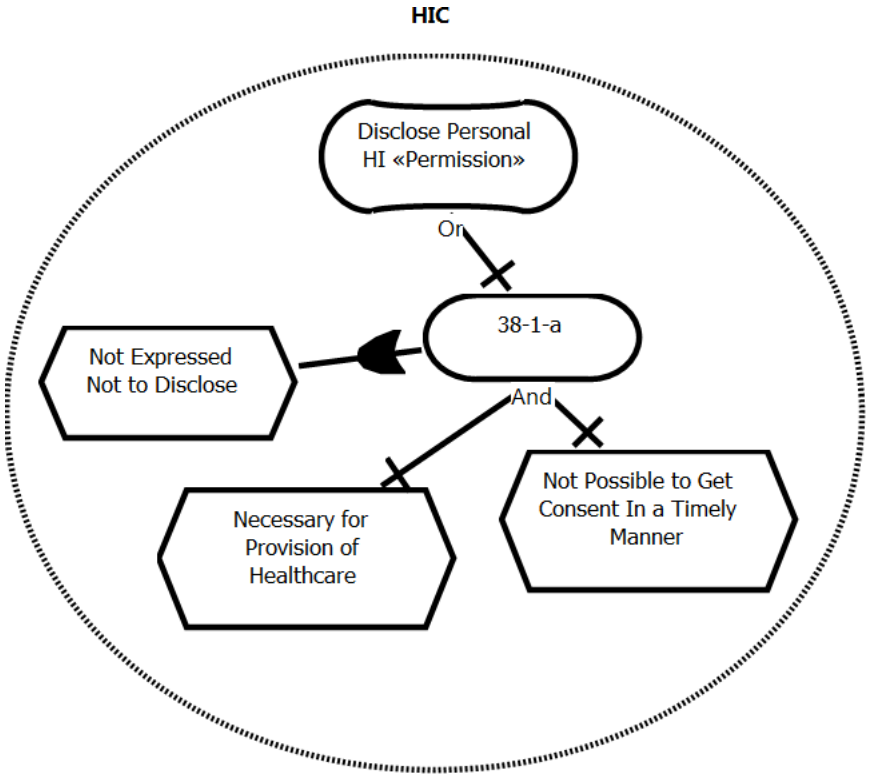

Figure C.26: PHIPA - Article 38 -1a

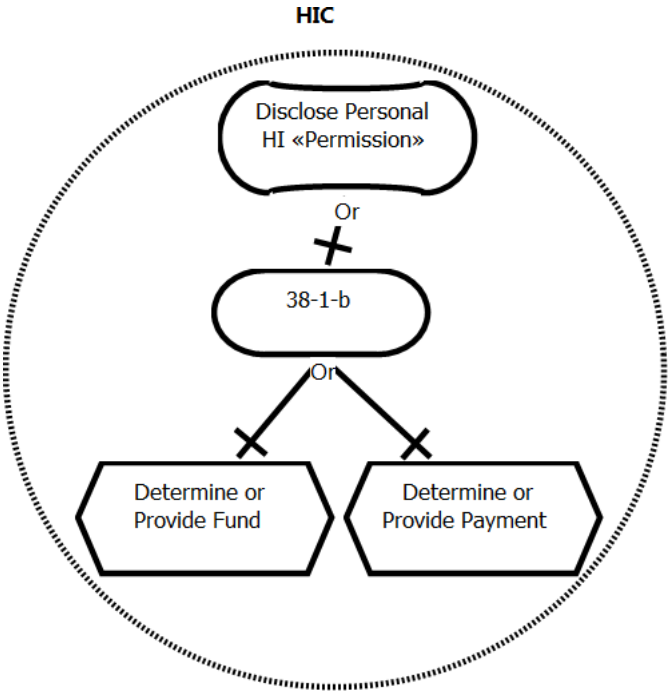

Figure C.27: PHIPA - Article 38 -1b

Notice of instruction

(2) If an HIC discloses PHI about an individual under clause (1) (a) and if an instruction of the individual made under that clause prevents the custodian from disclosing all the PHI that the custodian considers reasonably necessary to disclose for the provision of health care or assisting in the provision of health care to the individual, the custodian *shall* notify the person to whom it makes the disclosure of that fact. → Duty-Claim Statement → Obligation Goal. See Table C.19) and Figure C.29.

Facility that provides health care

(3) An HIC that is a facility that provides health care *may* disclose to a person the following PHI relating to an individual who is a patient or a resident in the facility if the custodian offers the individual the option, at the first reasonable opportunity after admission to the facility, to object to such disclosures and if the individual does not do so: → Privilege-NoClaim Statement → Permission Goal.

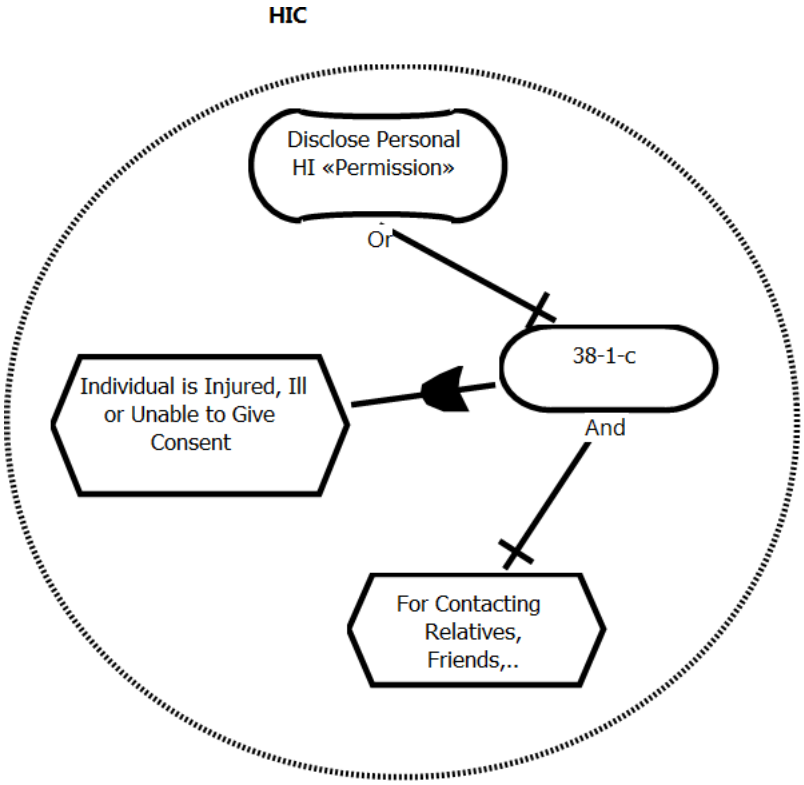

Figure C.28: PHIPA - Article 38 - 1c

1. The fact that the individual is a patient or resident in the facility.

2. The individual's general health status described as critical, poor, fair, stable or satisfactory, or in similar terms.

3. The location of the individual in the facility. (Table C.20)

Deceased individual

(4) An HIC *may* disclose PHI about an individual who is deceased, or is reasonably suspected to be deceased, → Privilege-NoClaim Statement → Permission Goal.

(a) for the purpose of identifying the individual;

(b) for the purpose of informing any person whom it is reasonable to inform in the circumstances of,

(i) the fact that the individual is deceased or reasonably suspected to be deceased,

Table C.19: PHIPA-Article 38 (2)

Section	Disclosures Related to Providing Health Care
Actor	An HIC
Modal Verb	Shall
Clause	Notify the person to whom it makes the disclosure of that fact.
Precondition 1	If an HIC discloses PHI about an individual under clause (1) (a) and
Precondition 2	If an instruction of the individual made under that clause prevents the custodian from disclosing all the PHI that the custodian considers reasonably necessary [...]

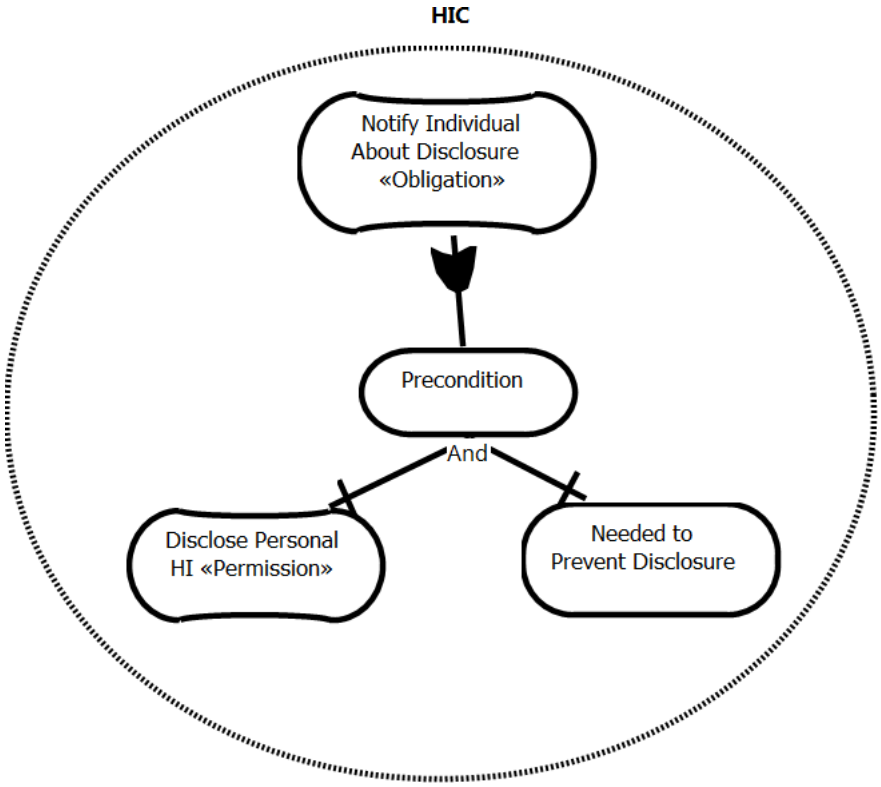

Figure C.29: PHIPA - Article 38 -2

and

(ii) the circumstances of death, where appropriate; or

(c) to the spouse, partner, sibling or child of the individual if the recipients of the information reasonably require the information to make decisions about their own health care or their children's health care. (Table C.21) and Figure C.30)

Table C.20: PHIPA-Article 38 (3)

Section	Disclosures Related to Providing Health Care
Actor	An HIC
Precondition 1	That is a facility that provides health care
Modal Verb	May
Clause	Disclose to a person the following PHI relating to an individual who is a patient or a resident in the facility
Precondition 2	If the custodian offers the individual the option [...]
Precondition 3	if the individual does not do so: 1-3

Table C.21: PHIPA-Article 38 (4)

Section	Disclosures Related to Providing Health Care
Actor	An HIC
Modal Verb	May
Clause	Disclose PHI about an individual who is deceased, or is reasonably suspected to be deceased for a-c

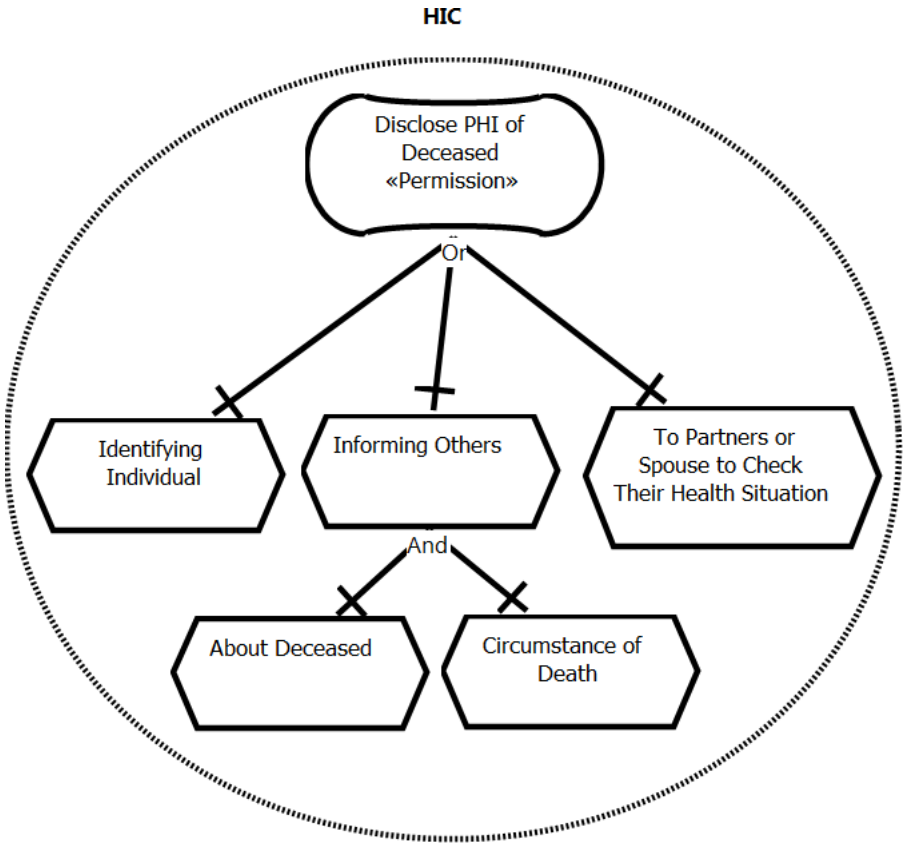

Figure C.30: PHIPA - Article 38-4

C.8 Article 44 - Disclosure for Research

44. (1) An HIC *may* disclose PHI about an individual to a researcher if the researcher, → Privilege-NoClaim Statement → Permission Goal.

(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).

Table C.22 summarizes the statement's parts and Figure C.31 shows the Articles 44(1) and (5) modeled in Legal GRL.

Table C.22: PHIPA-Article 44 (1)(5)

Section	Disclosure for research
Actor	An HIC
Modal Verb	May
Clause 1	Disclose PHI about an individual to a researcher if the researcher
Precondition 1	Submits to the custodian [...]
Precondition 2	Enters into the agreement required by subsection
Precondition	-
Exception	-

Research plan

(2) A research plan *must* be in writing and must set out, → Duty-Claim Statement → Obligation Goal.

(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. (Table C.23 and Figure C.32)

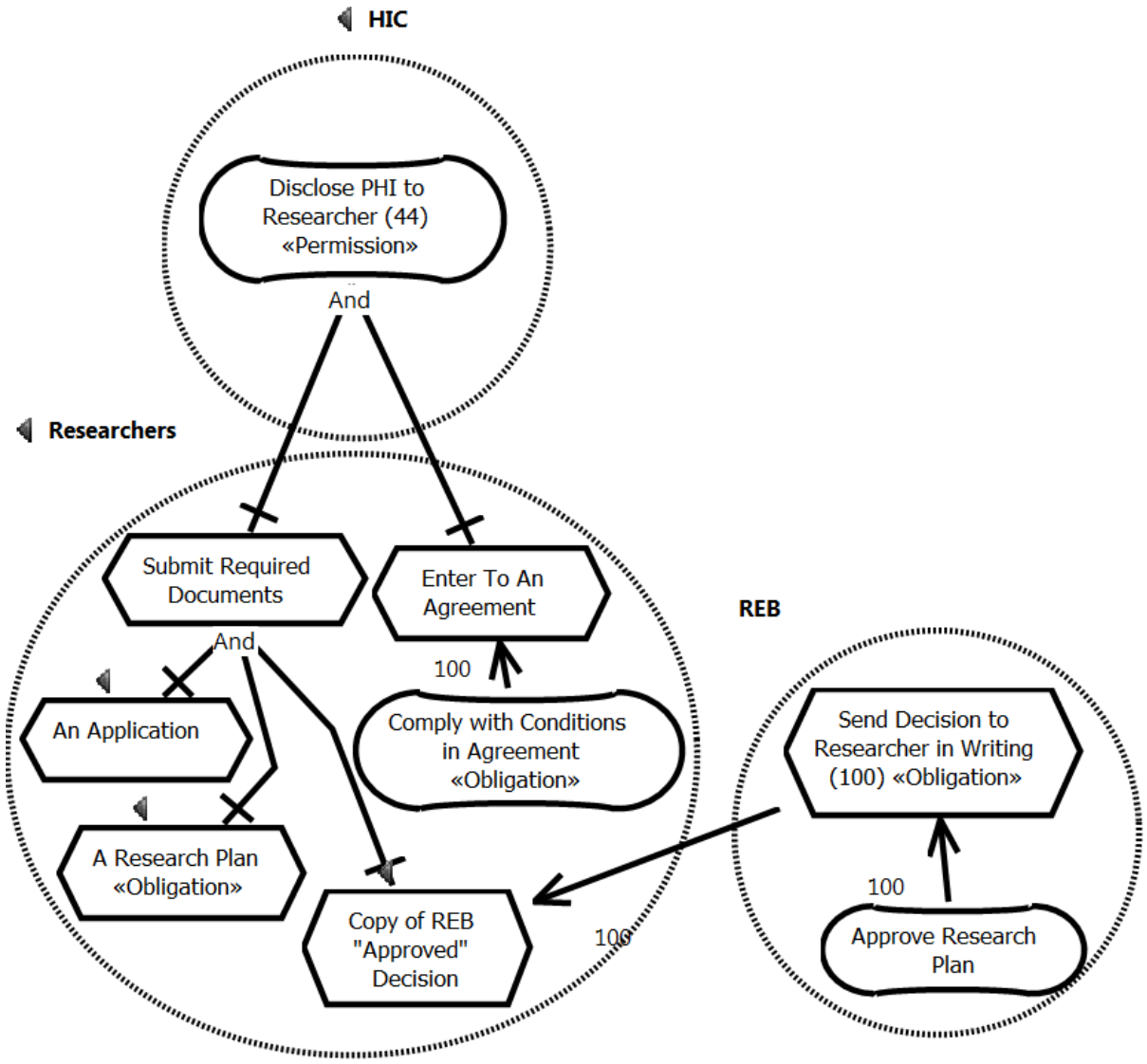

Figure C.31: PHIPA - Article 44(1)

Table C.23: PHIPA-Article 44 (2)

Section	Disclosure for research
Actor	A Research plan
Modal Verb	Must
Clause	Be in writing and set out [...]
Precondition	-
Exception	-

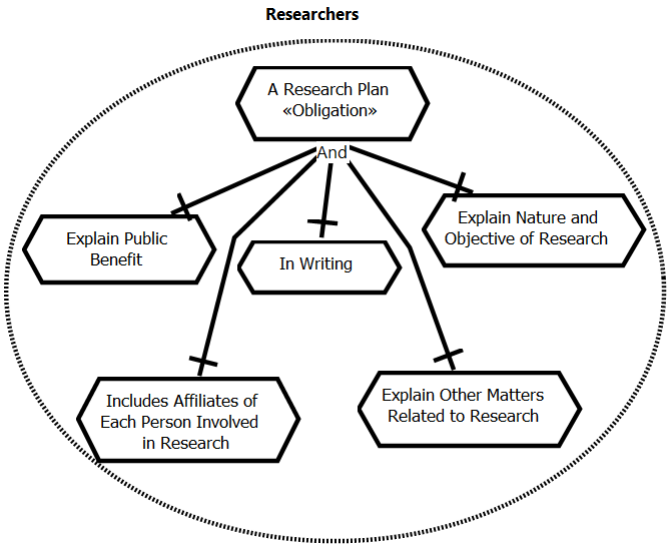

Figure C.32: PHIPA - Article 44(2)

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, → Duty-Claim Statement → Obligation Goal.

(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 PHI 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. (Table C.24 and Figure C.33)

Table C.24: PHIPA-Article 44 (3)

Section	Disclosure for research
Actor	A Research Ethic Board
Modal Verb	Shall
Clause	Consider the matters that it considers relevant, including (a) to (d)
Precondition	When deciding whether to approve a research plan that a researcher submits to it
Exception	-

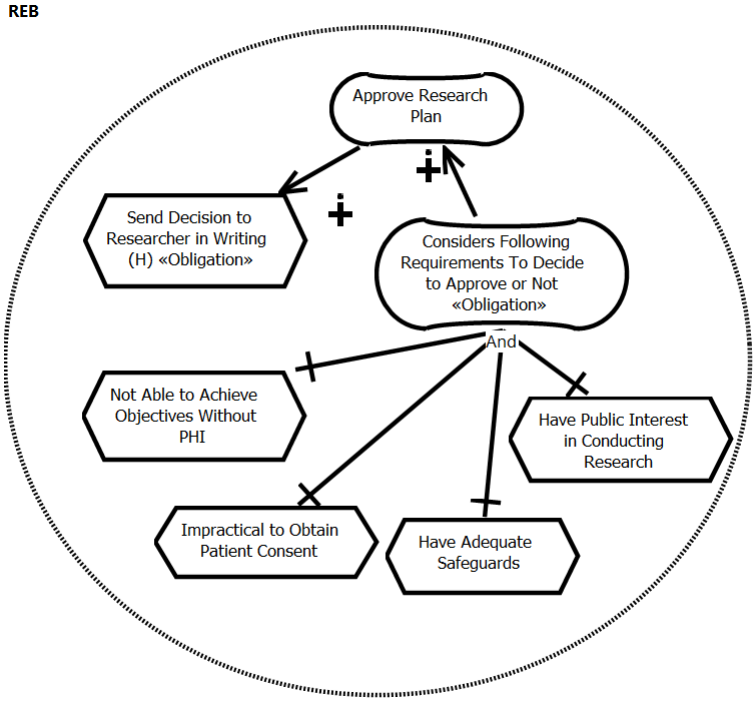

Figure C.33: PHIPA - Article 44(3) - (4)

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. → Duty-Claim Statement → Obligation Goal. See Table C.25 and Figure C.33.

Table C.25: PHIPA-Article 44 (4)

Section	Disclosure for research
Actor	The Research Ethic Board
Modal Verb	Shall
Clause	Provide to the researcher a decision in writing, with reasons, [...]
Precondition	-
Exception	-

Agreement respecting disclosure

(5) Before an HIC discloses PHI 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. → Duty-Claim Statement → Obligation Goal. See Table C.26.

Table C.26: PHIPA-Article 44 (5)

Section	Disclosure for research
Actor	The researcher
Modal Verb	Shall
Clause	enter into an agreement with the custodian in which the researcher [...]
Precondition	-
Exception	-

Compliance by researcher

(6) A researcher who receives PHI about an individual from an HIC under subsection (1) *shall*, → Duty-Claim Statement → Obligation Goal.

(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). (Table C.27 and Figure C.34)

Table C.27: PHIPA-Article 44 (6)

Section	Disclosure for research
Actor	A researcher
Modal Verb	Shall
Clause	Comply with the conditions, [...], (b) - (g)
Precondition	-
Exception	-

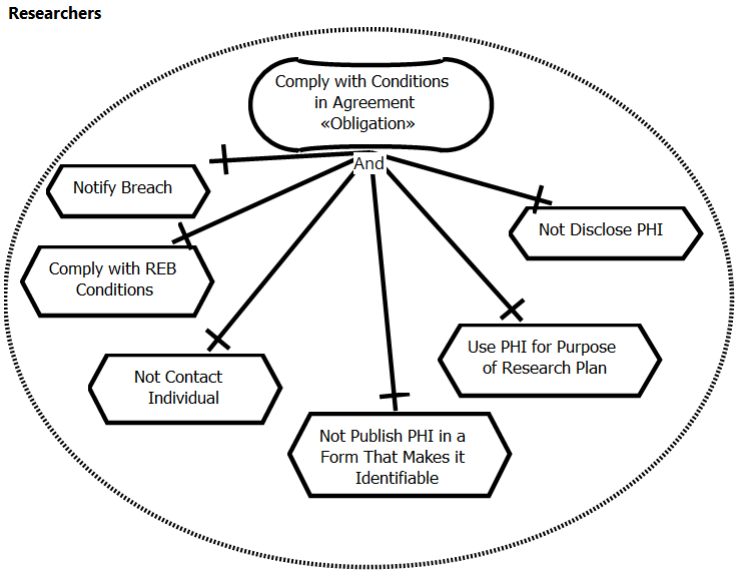

Figure C.34: PHIPA - Article 44(6)

Appendix D

The Ontario Hospital GRL and UCM Models and Legal Compliance Analysis

This appendix presents the models related to the hospital, together with the other 8 views of the legal-organizational GRL model as well as the quantitative and qualitative analysis of these models.

D.1 Hospital - Disclose PHI to Hospital Employees

Figure D.1 shows the GRL model for the case where the hospital discloses PHI to its employees for providing better healthcare.

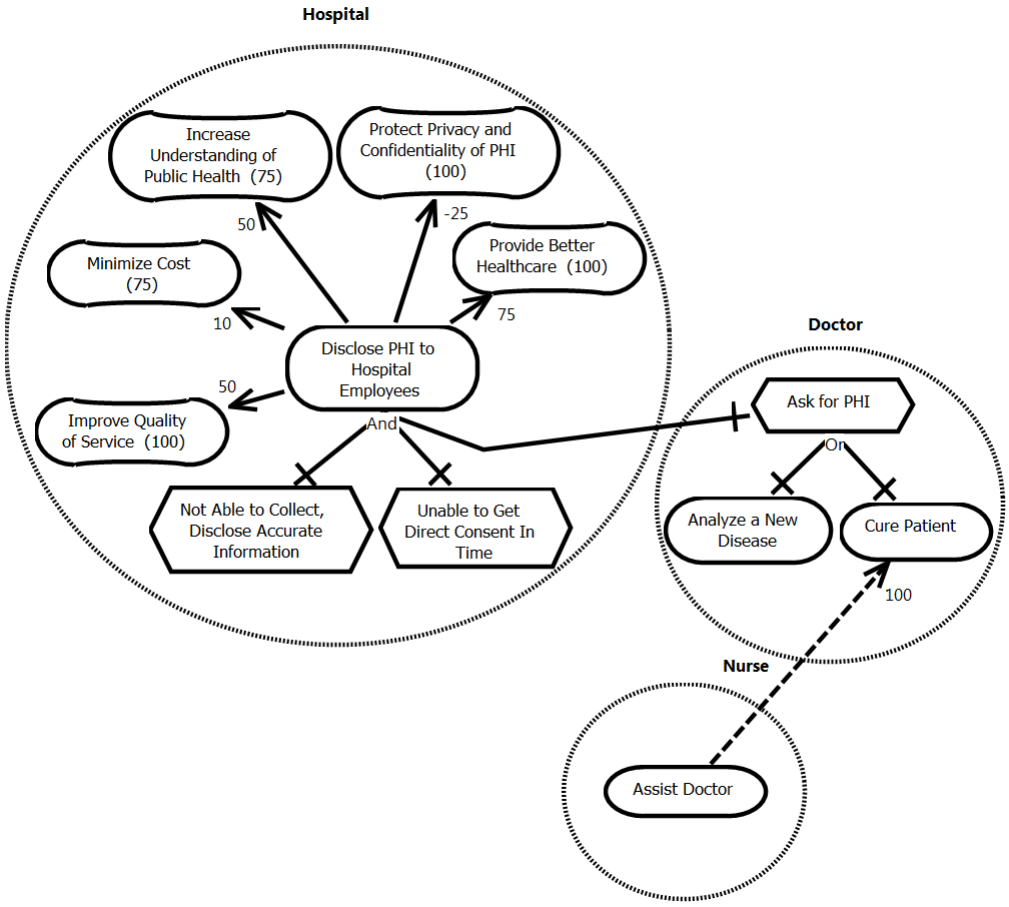

Figure D.1: Hospital - Disclose to a Hospital Employee Goal Model

D.2 Hospital - Disclose PHI for Payment or Claims

Figure D.2 shows the GRL model for the case where the hospital discloses PHI to its employees for obtaining payment or monitoring, verifying or reimbursing a claim.

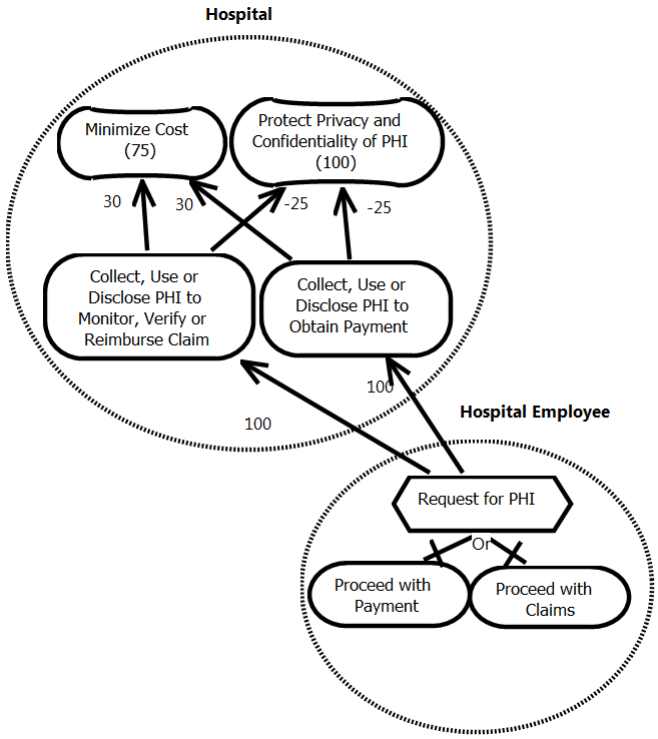

Figure D.2: Hospital - Disclose For Payment or Claims Goal Model

D.3 Hospital - Disclose PHI for Investigating Breaching

Figure D.3 shows the GRL model for the case where the hospital discloses PHI to a legal agency for investigating a breach. In this case, the legal agency requests access to PHI to investigate the researcher's breach.

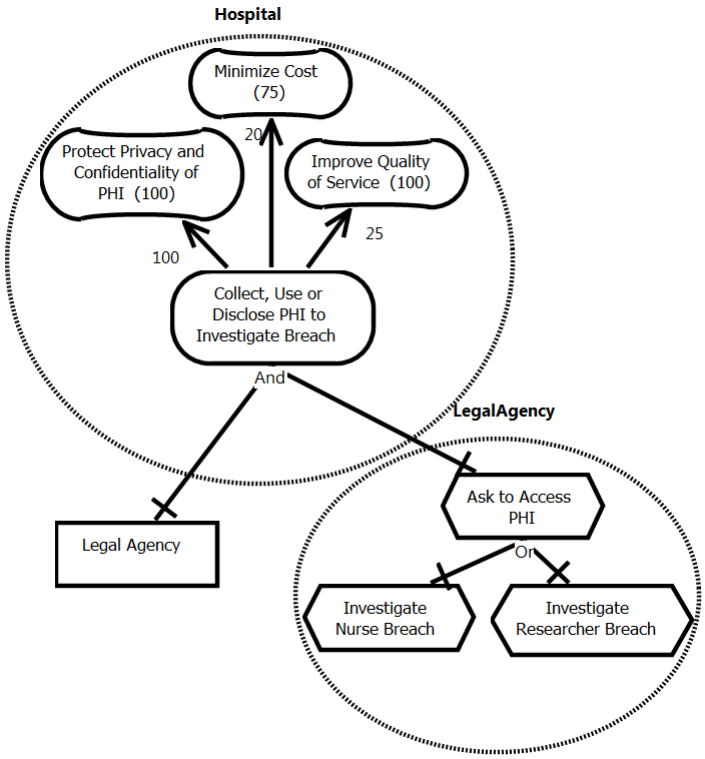

Figure D.3: Hospital - Disclose For Investigating a Breach Goal Model

D.4 Organizational and Legal GRL Models

In this section, the 9 Legal-Organizational models built for the hospital are shown.

Disclose PHI to Healthcare Providers

Figure D.4 and Figure D.5 present the organizational-legal model for disclosing PHI for providing healthcare.

Disclose PHI to Hospital for Payment

Figure D.6 presents the organizational-legal model for disclosing PHI to the hospital for processing the payment.

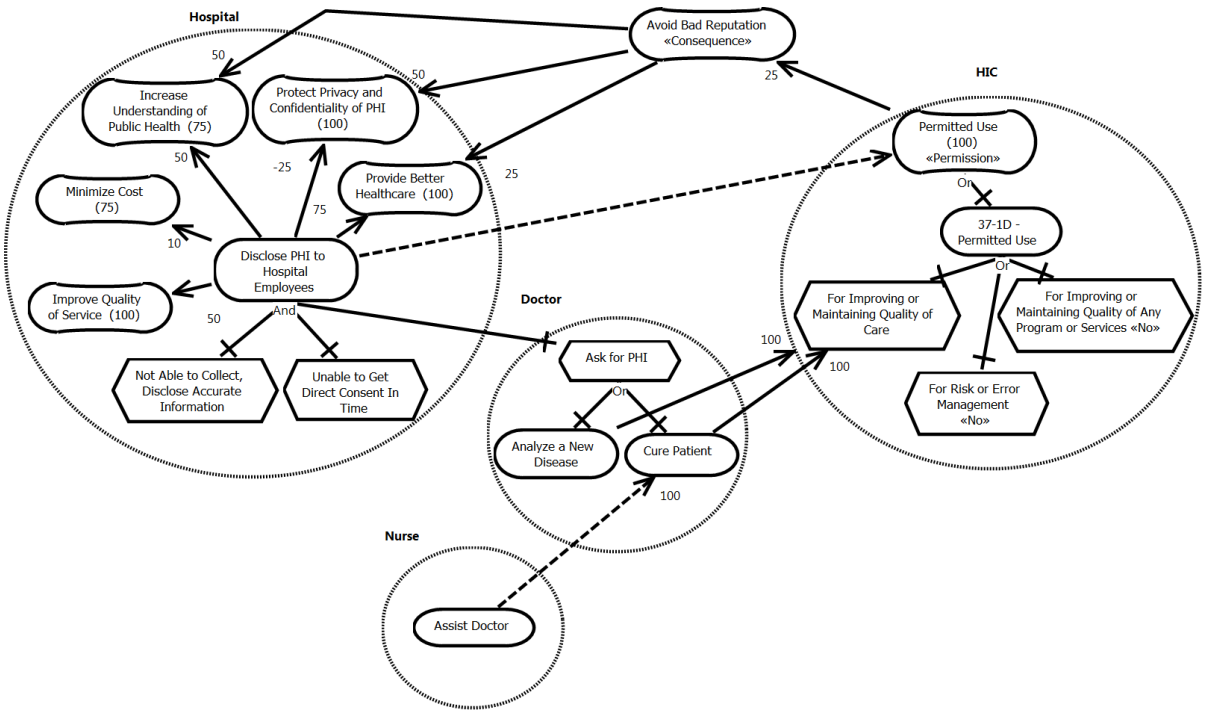

Figure D.4: Disclose PHI to Healthcare Providers(1)

Disclose PHI to Hospital for Breach

Figure D.7 and Figure D.8 present the organizational-legal model for disclosing PHI to the hospital to investigate a breach.

Disclose PHI to Researchers

Figure D.9, Figure D.10, Figure D.11 and Figure D.12 present the organizational-legal model for disclosing PHI to researchers.

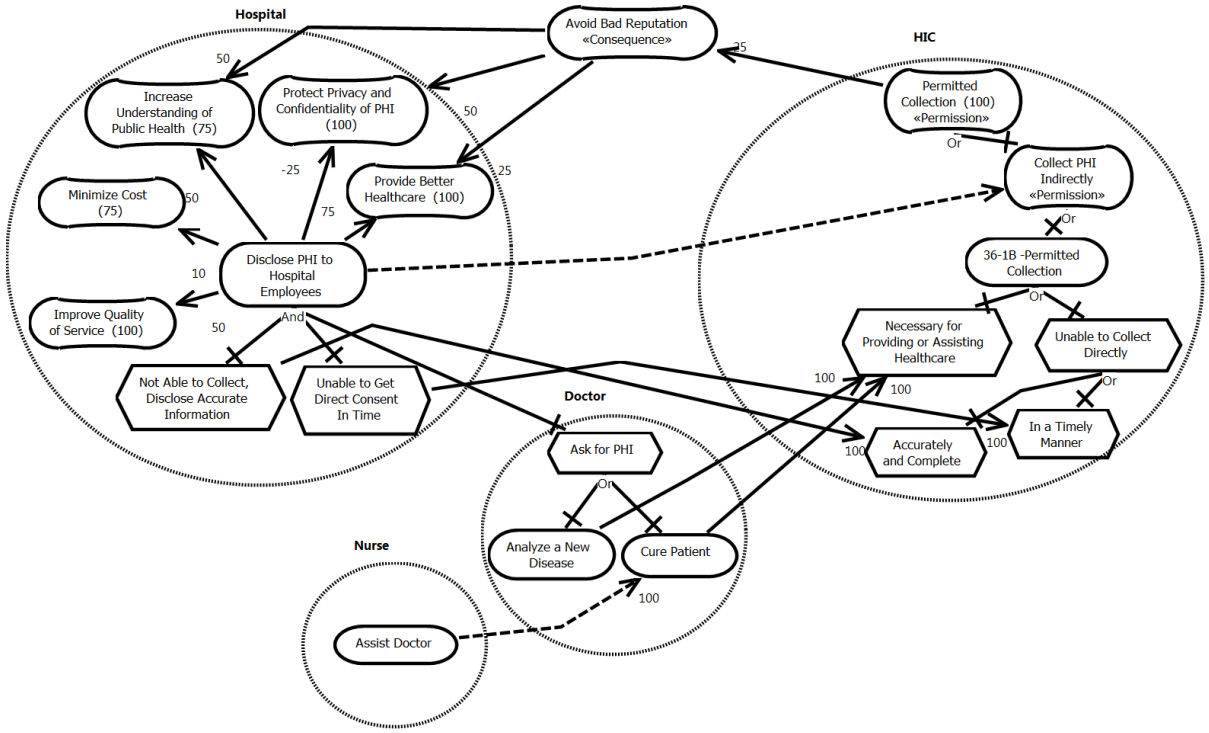

Figure D.5: Disclose PHI to Healthcare Providers (2)

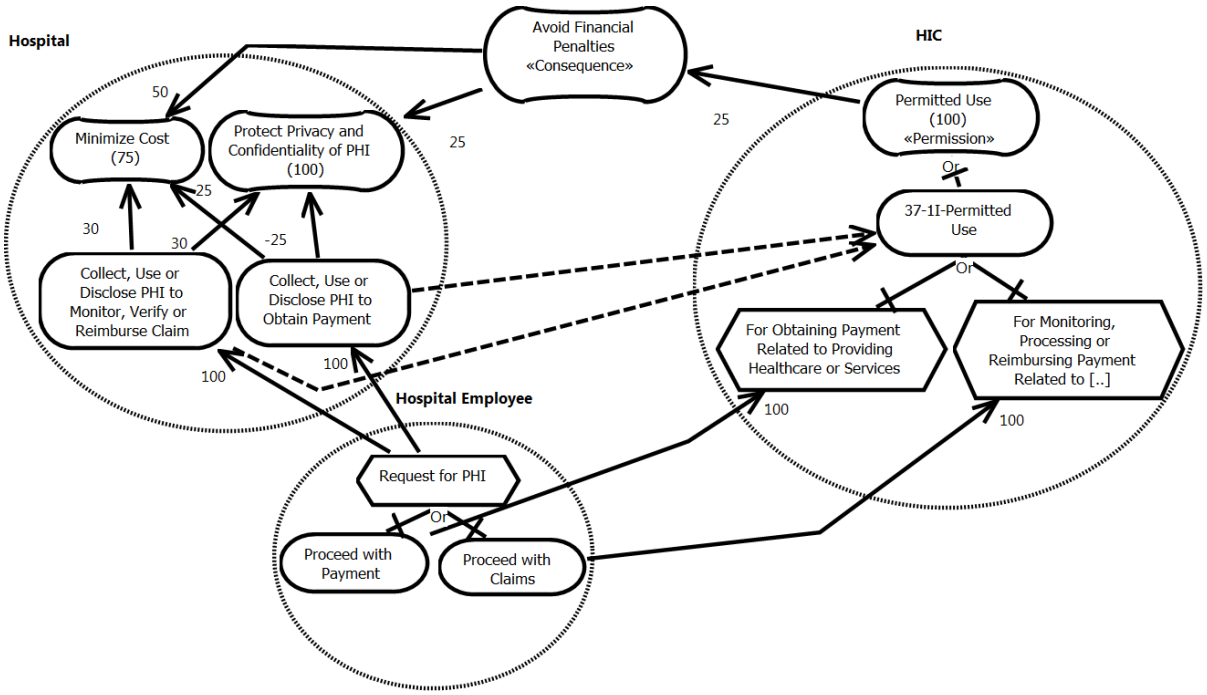

Figure D.6: Disclose PHI to Hospital for Payment

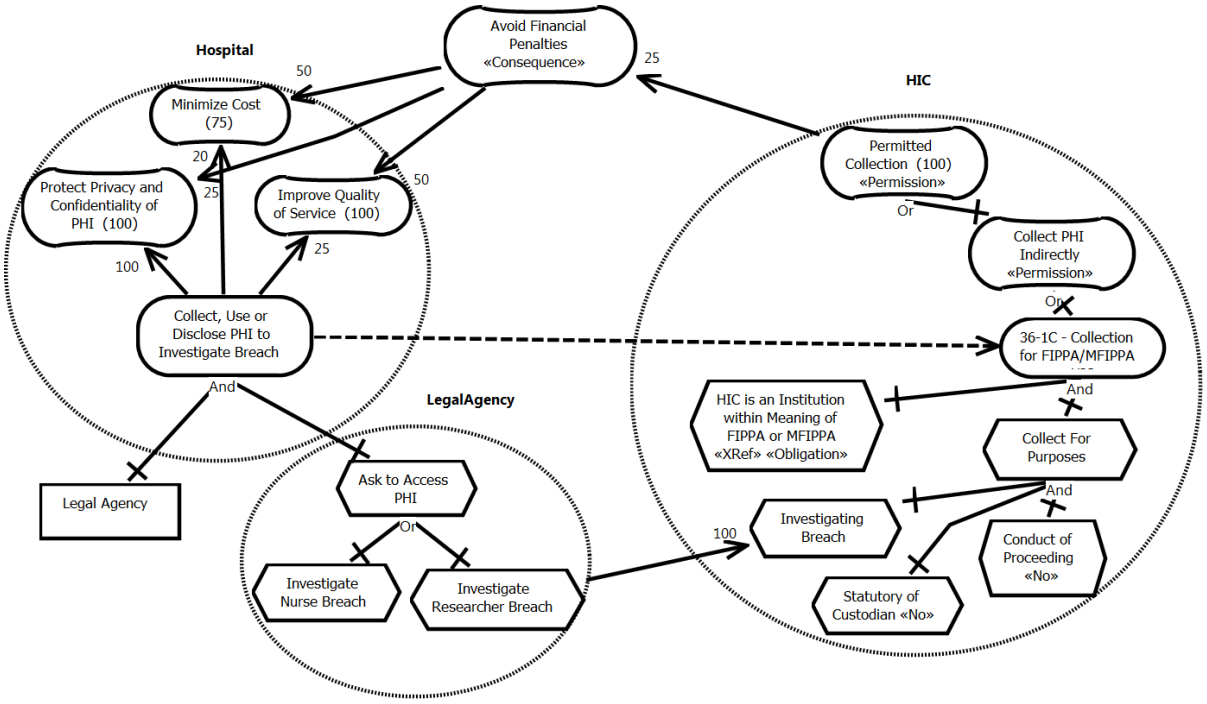

Figure D.7: Disclose PHI to Hospital for Investigating Breach (1)

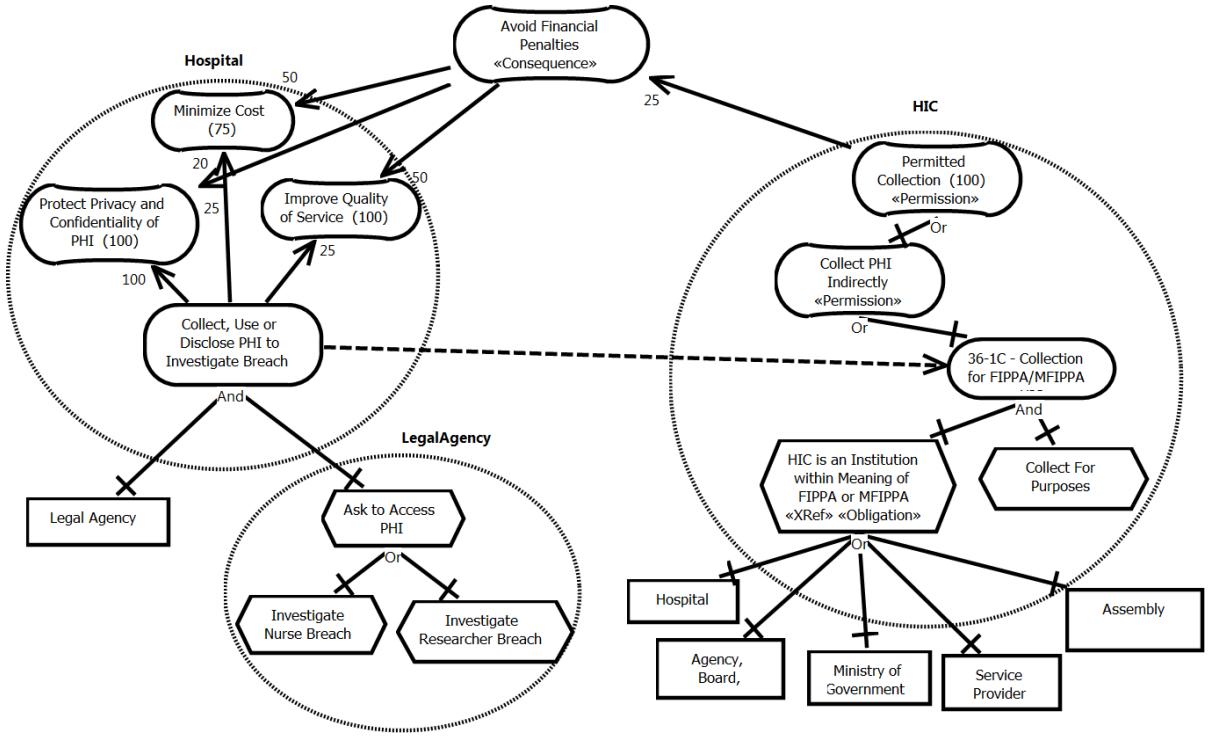

Figure D.8: Disclose PHI to Hospital for Investigating Breach (2)

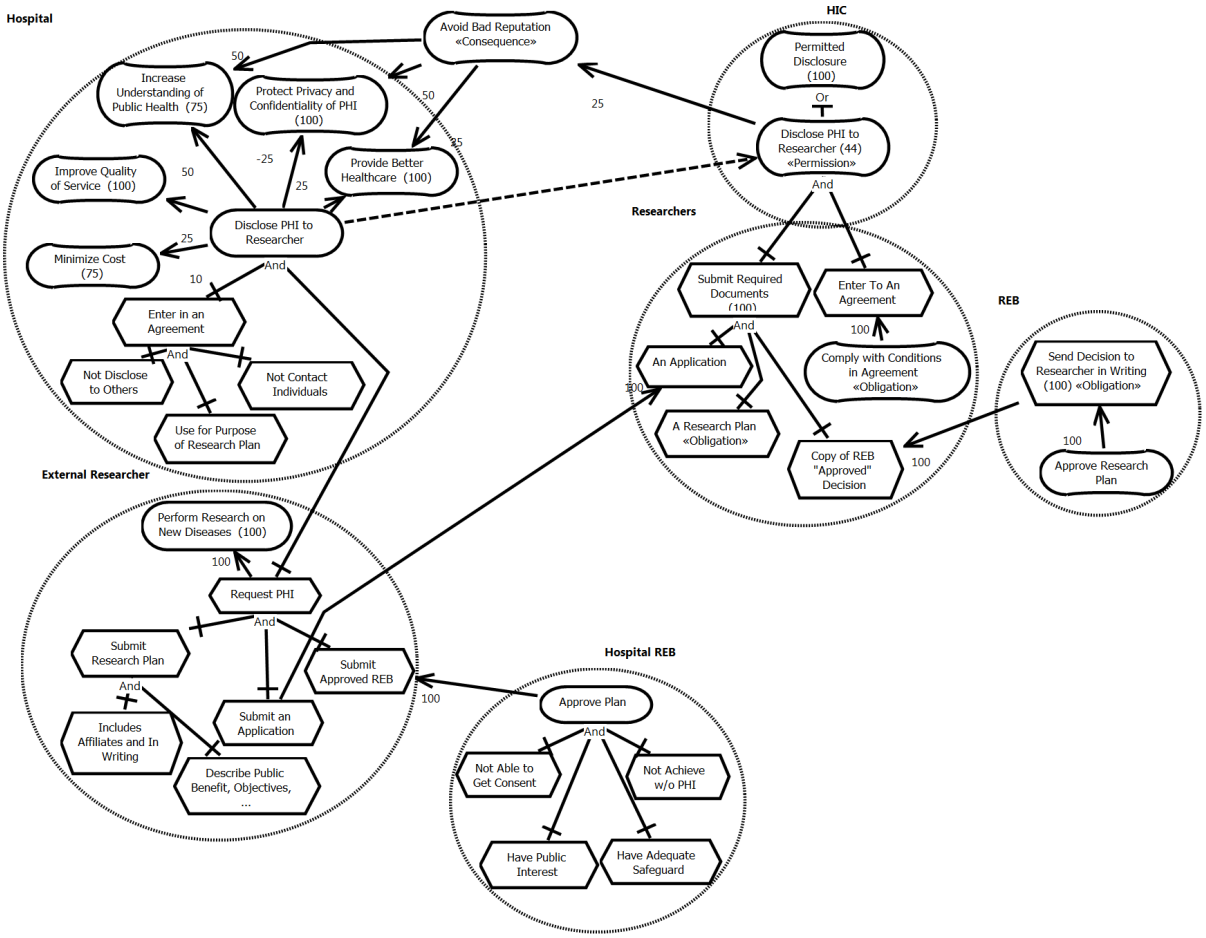

Figure D.9: Disclose PHI to Researchers (1)

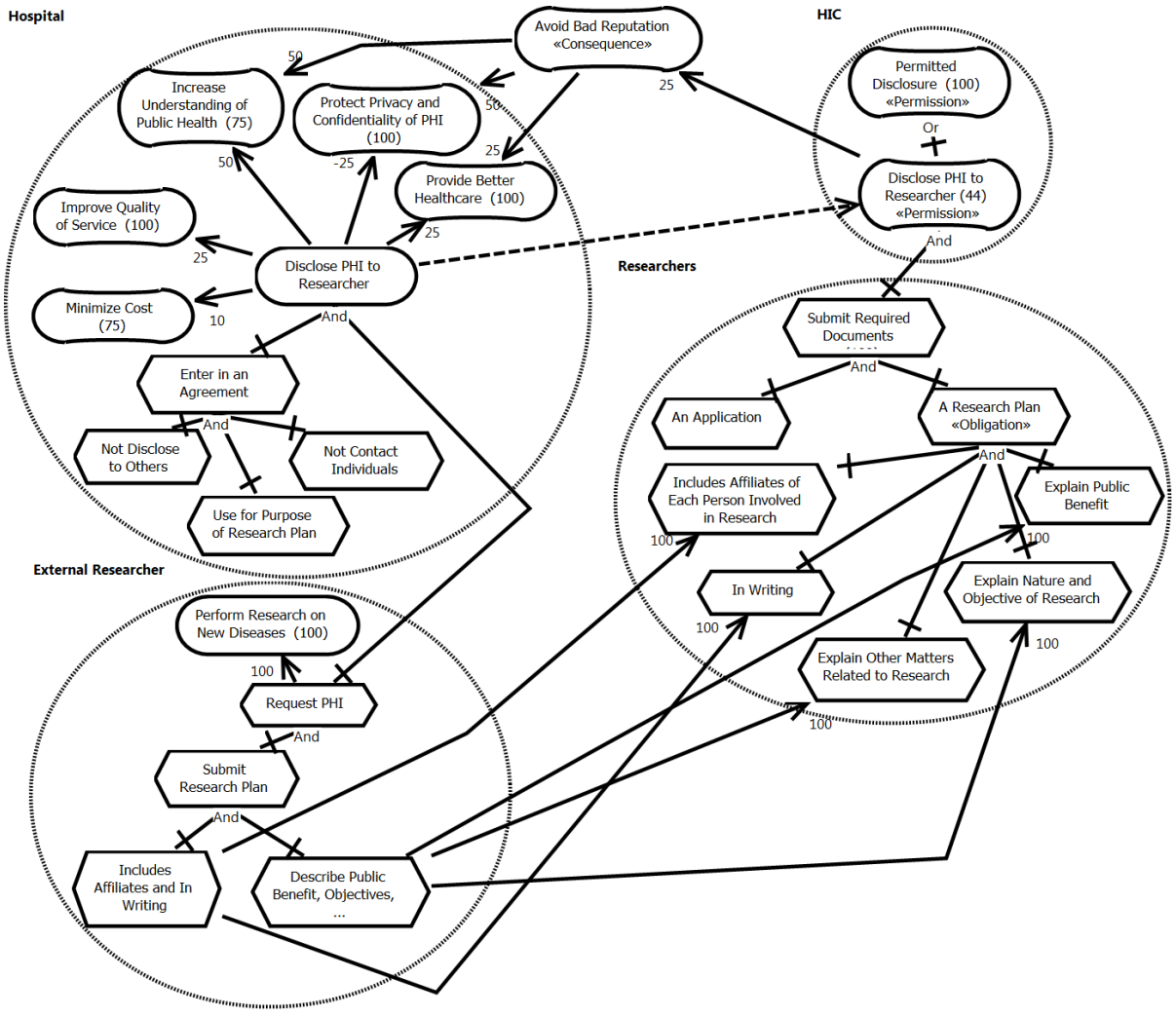

Figure D.10: Disclose PHI to Researchers (2)

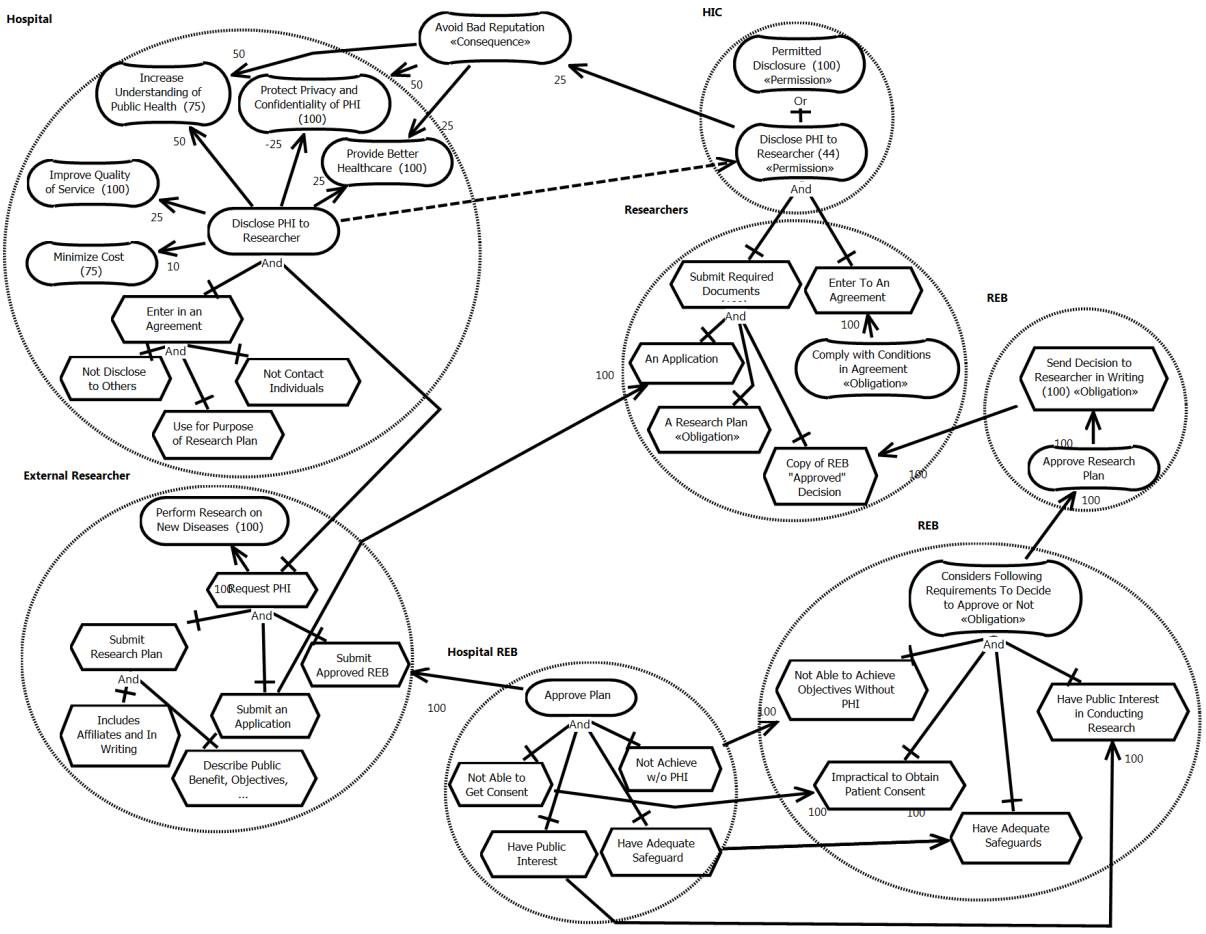

Figure D.11: Disclose PHI to Researchers (3)

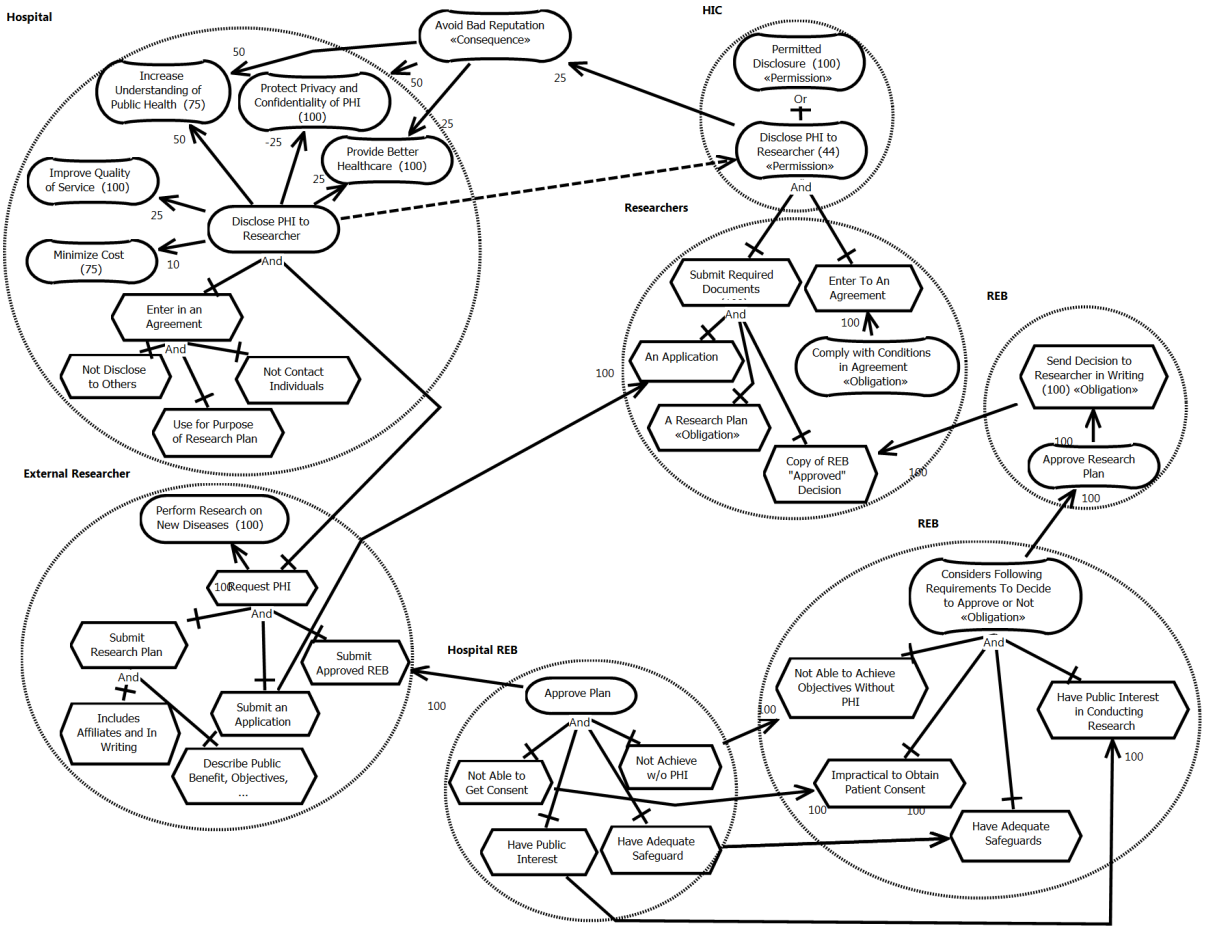

Figure D.12: Disclose PHI to Researchers (4)

D.5 Quantitative Analysis of the Models for the Base Strategy

Quantitative Analysis of Disclose PHI to Healthcare Providers

Figure D.13 and Figure D.14 present the quantitative analysis (base strategy) for disclosing PHI for providing healthcare.

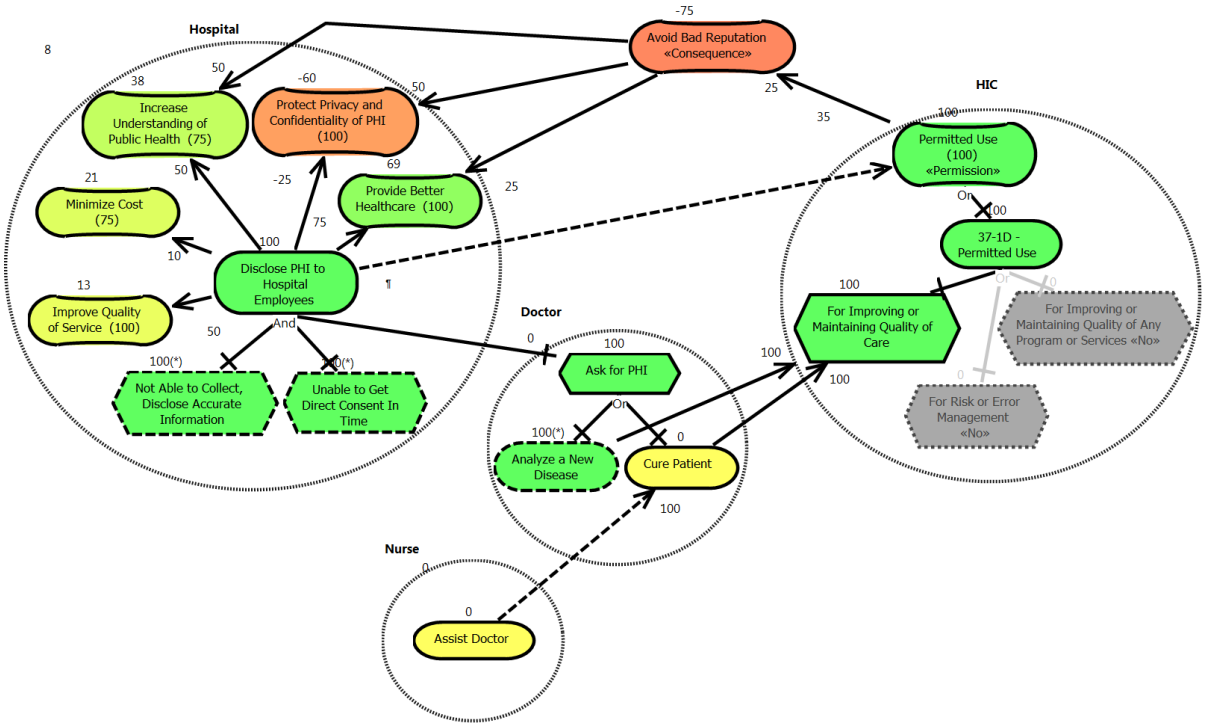

Figure D.13: Quantitative Analysis – Providing Healthcare (1)

Quantitative Analysis of Disclose PHI to Hospital for Payment

Figure D.15 presents the quantitative analysis (base strategy) for disclosing PHI for payment.

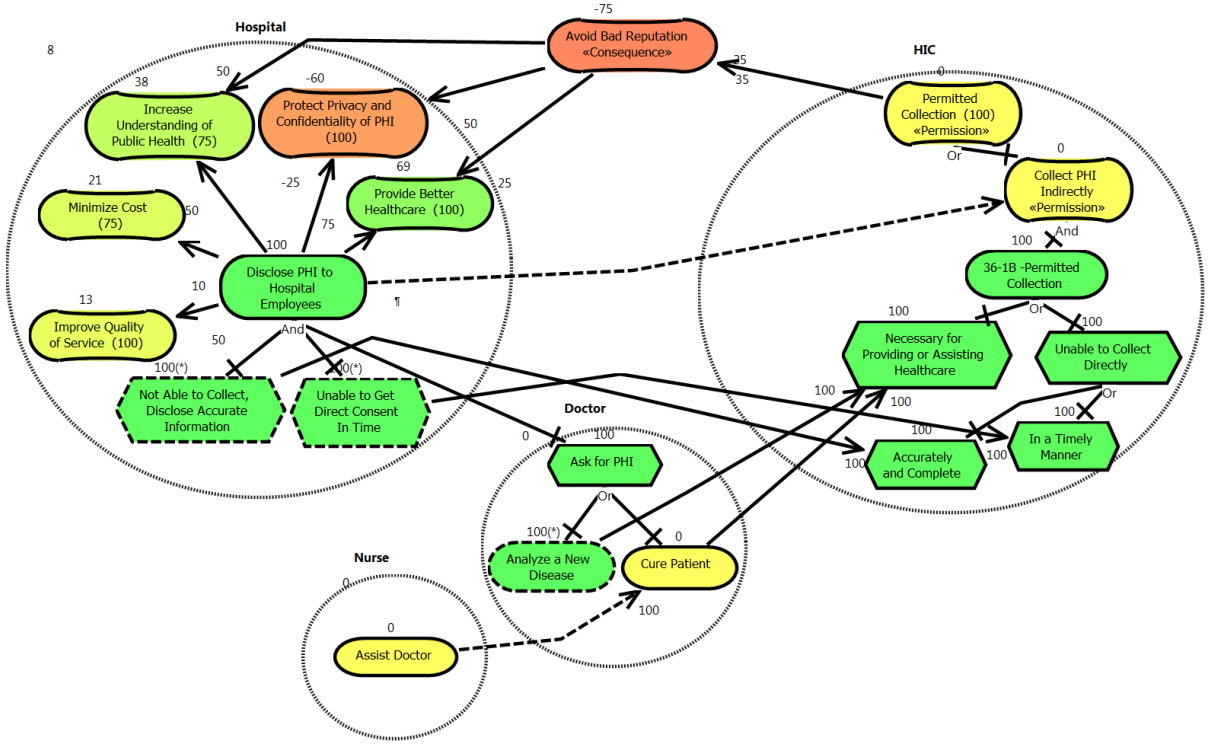

Figure D.14: Quantitative Analysis – Providing Healthcare (2)

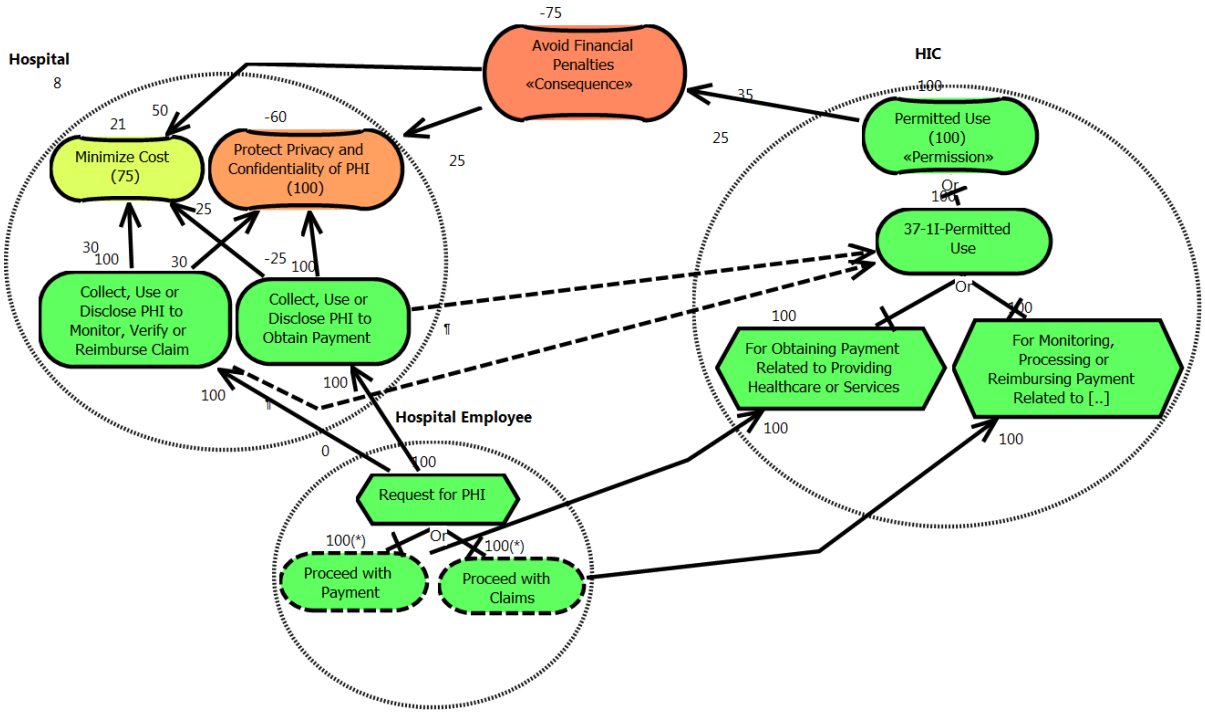

Figure D.15: Quantitative Analysis – Proceed a Payment

Quantitative Analysis of Disclose PHI to Hospital for Breach

Figure D.16 and Figure D.17 present the quantitative analysis (base strategy) for disclosing PHI for payment.

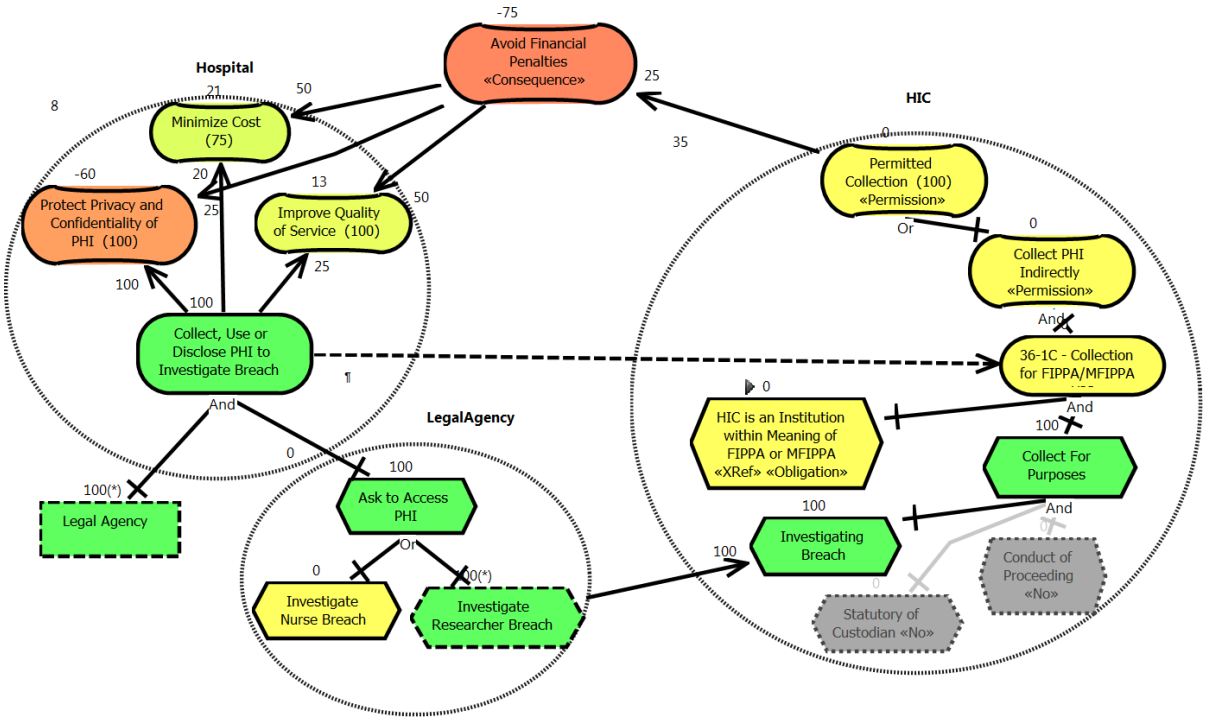

Figure D.16: Quantitative Analysis – Investigating Breach (1)

Quantitative Analysis Disclose PHI to Researchers

Figure D.18, Figure D.19, Figure D.20 and Figure D.21 present the quantitative analysis (base strategy) for disclosing PHI to researchers.

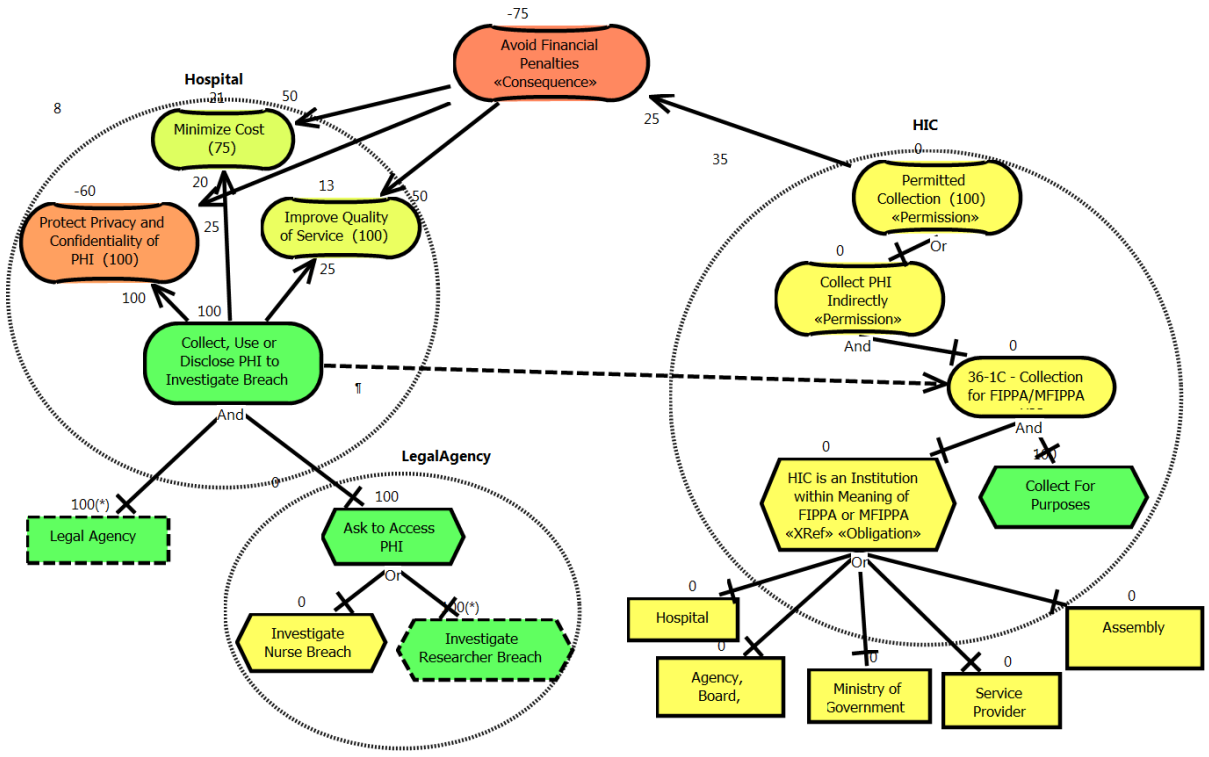

Figure D.17: Quantitative Analysis – Investigating Breach (2)

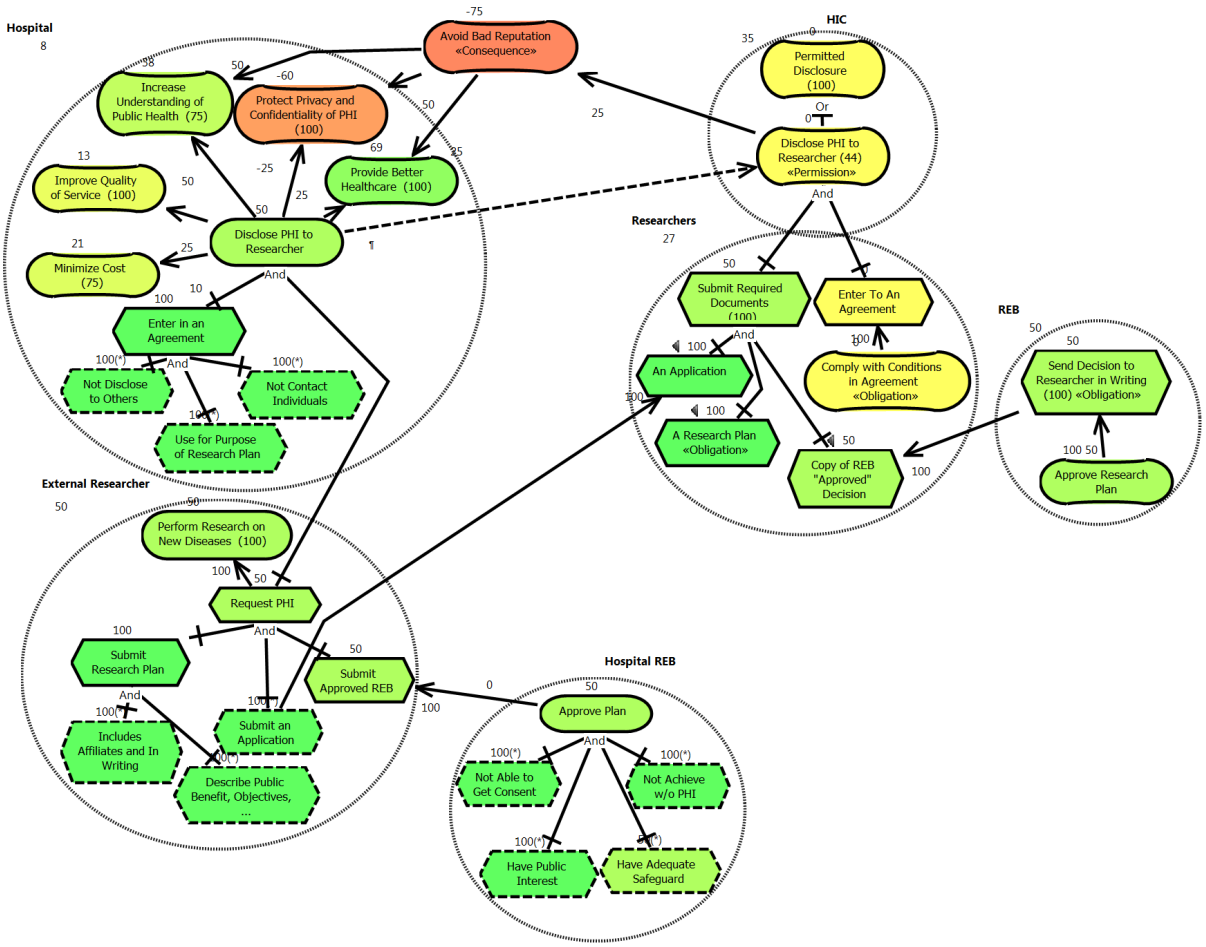

Figure D.18: Quantitative Analysis – Disclose to Researchers (1)

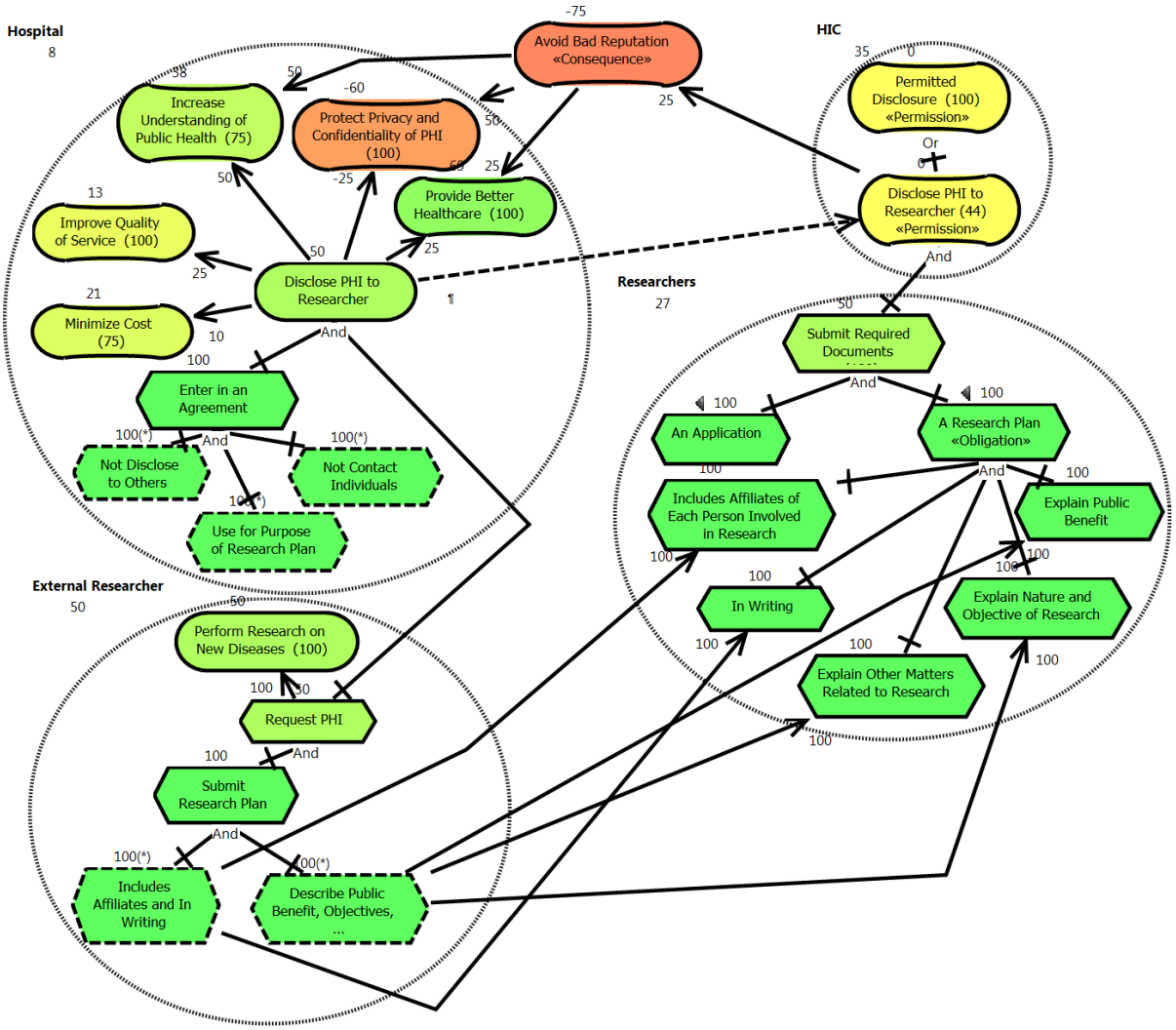

Figure D.19: Quantitative Analysis – Disclose to Researchers (2)

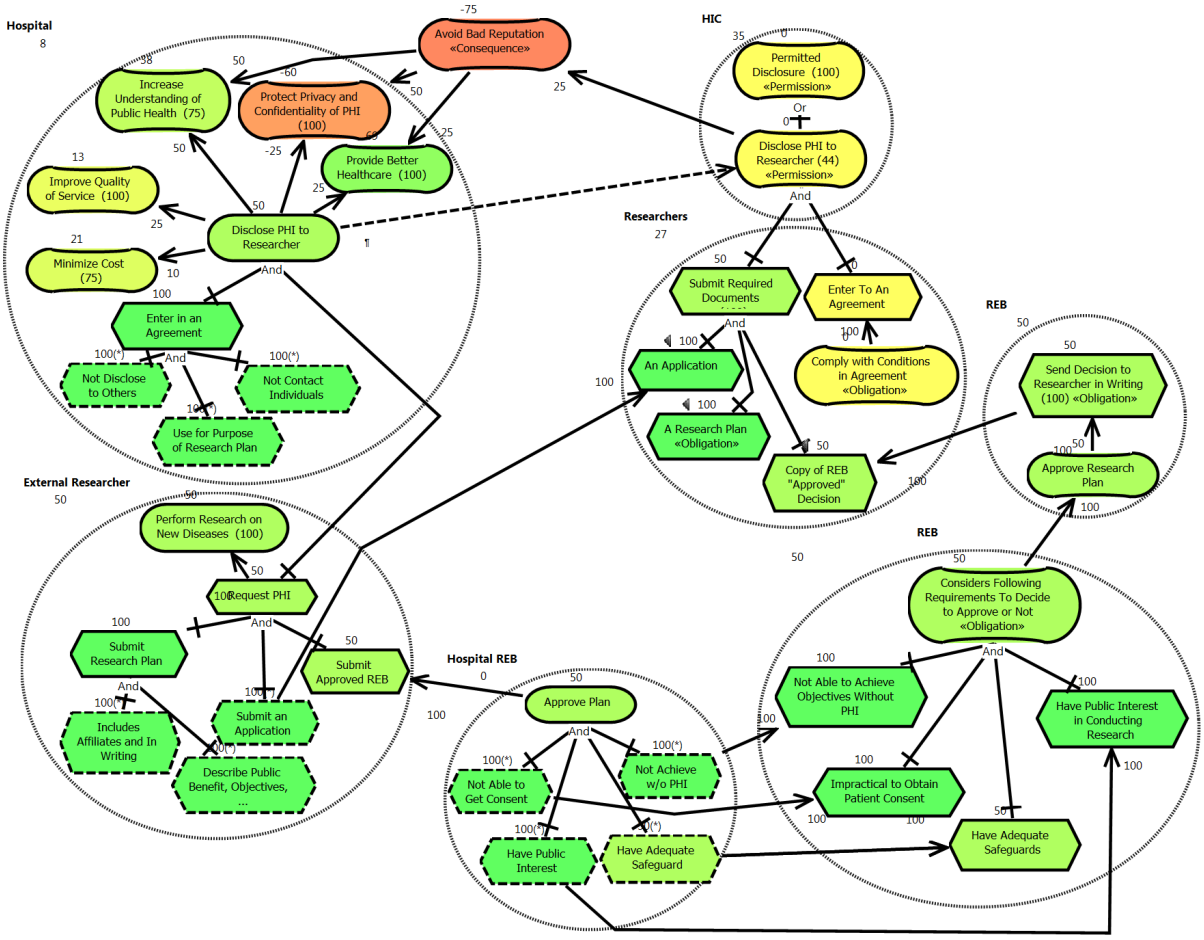

Figure D.20: Quantitative Analysis – Disclose to Researchers (3)

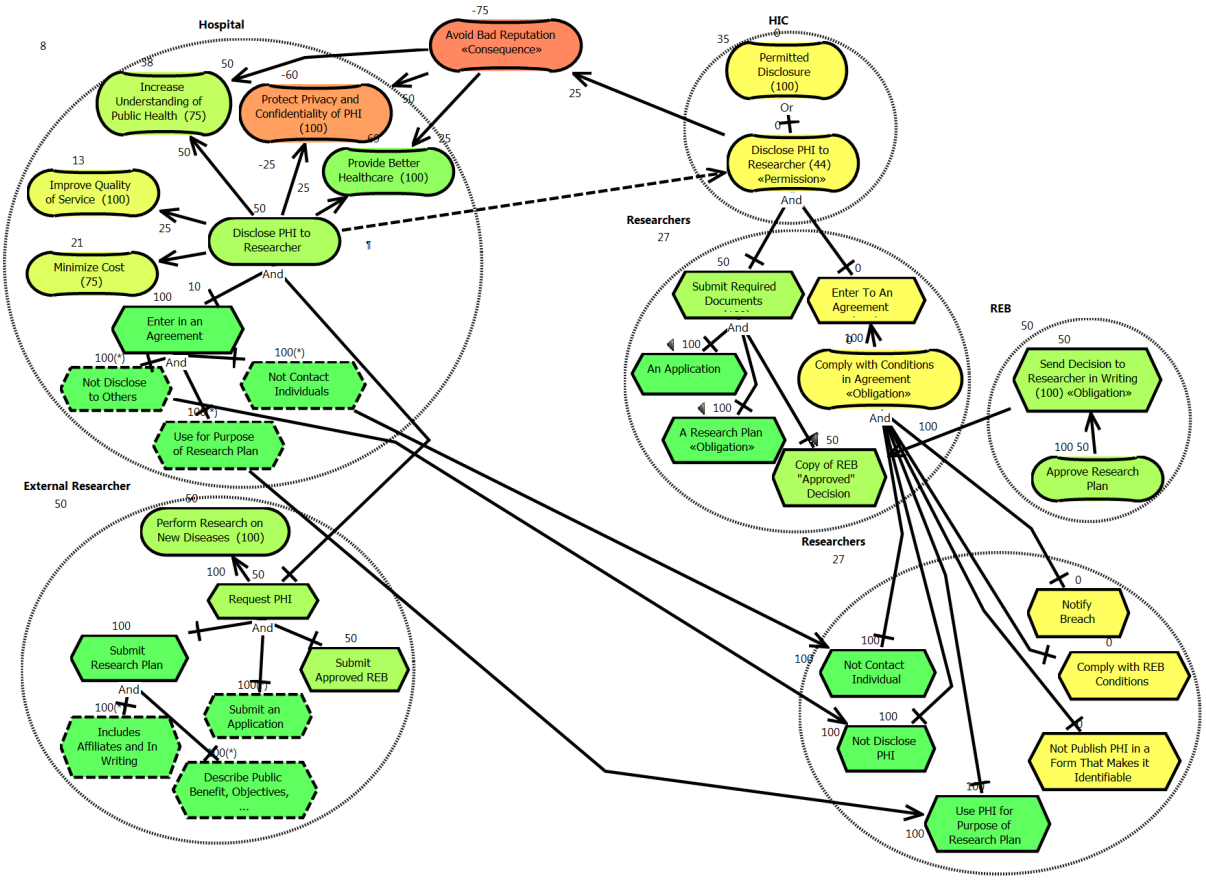

Figure D.21: Quantitative Analysis – Disclose to Researchers (4)

D.6 Qualitative Analysis of the Models for the Base Strategy

Qualitative Analysis of Disclose PHI to Healthcare Providers

Figure D.22 and Figure D.23 present the qualitative analysis (base strategy) for disclosing PHI for providing healthcare.

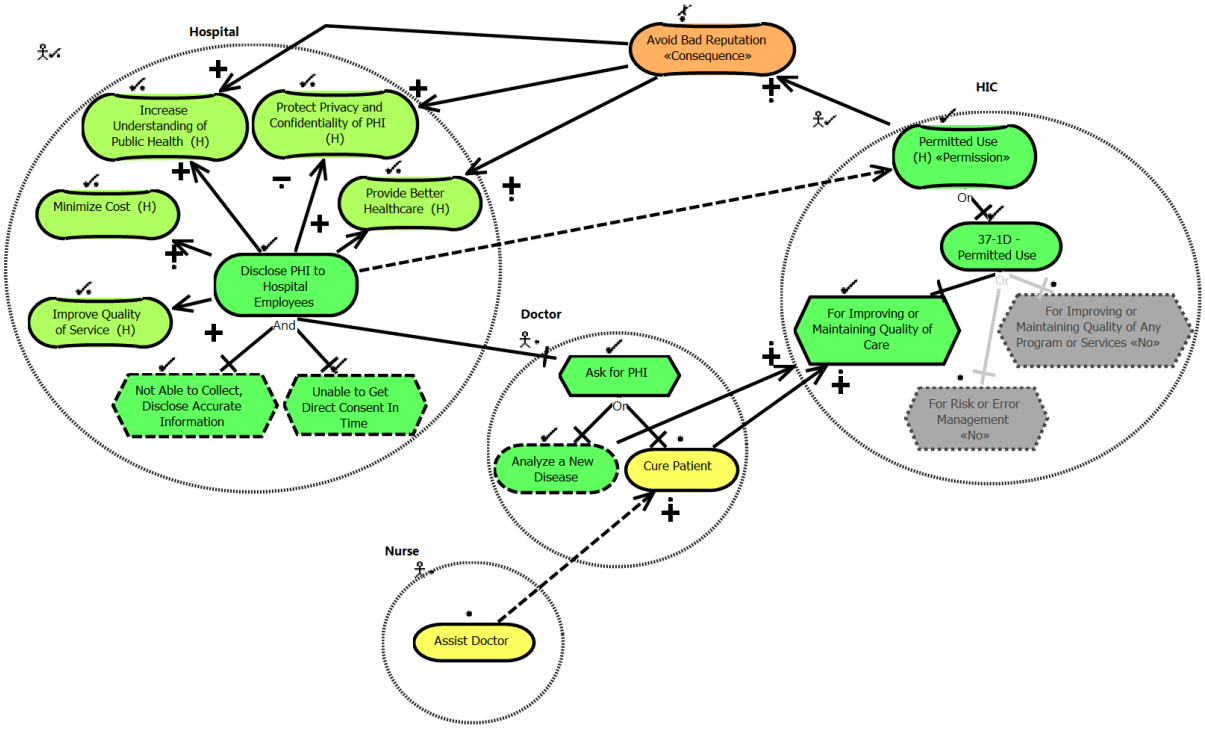

Figure D.22: Qualitative Analysis – Providing Healthcare (1)

Qualitative Analysis of Disclose PHI to Hospital for Payment

Figure D.24 presents the qualitative analysis (base strategy) for disclosing PHI for payment.

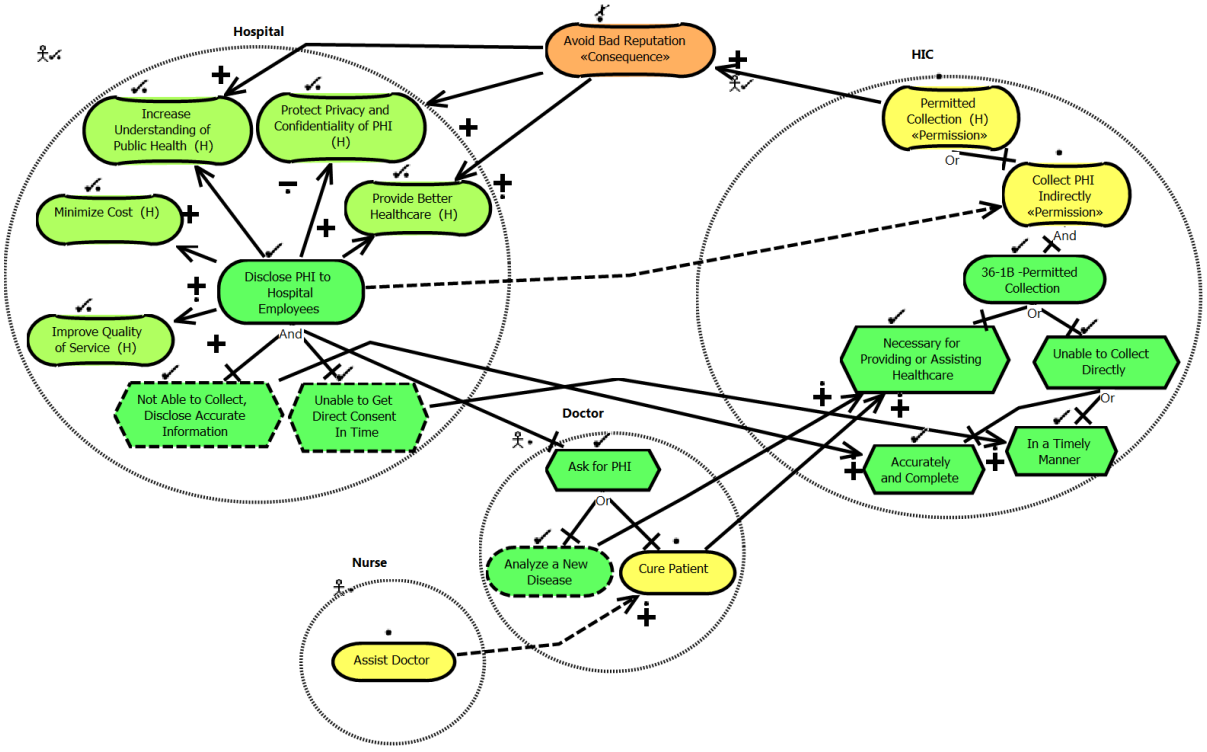

Figure D.23: Qualitative Analysis – Providing Healthcare (2)

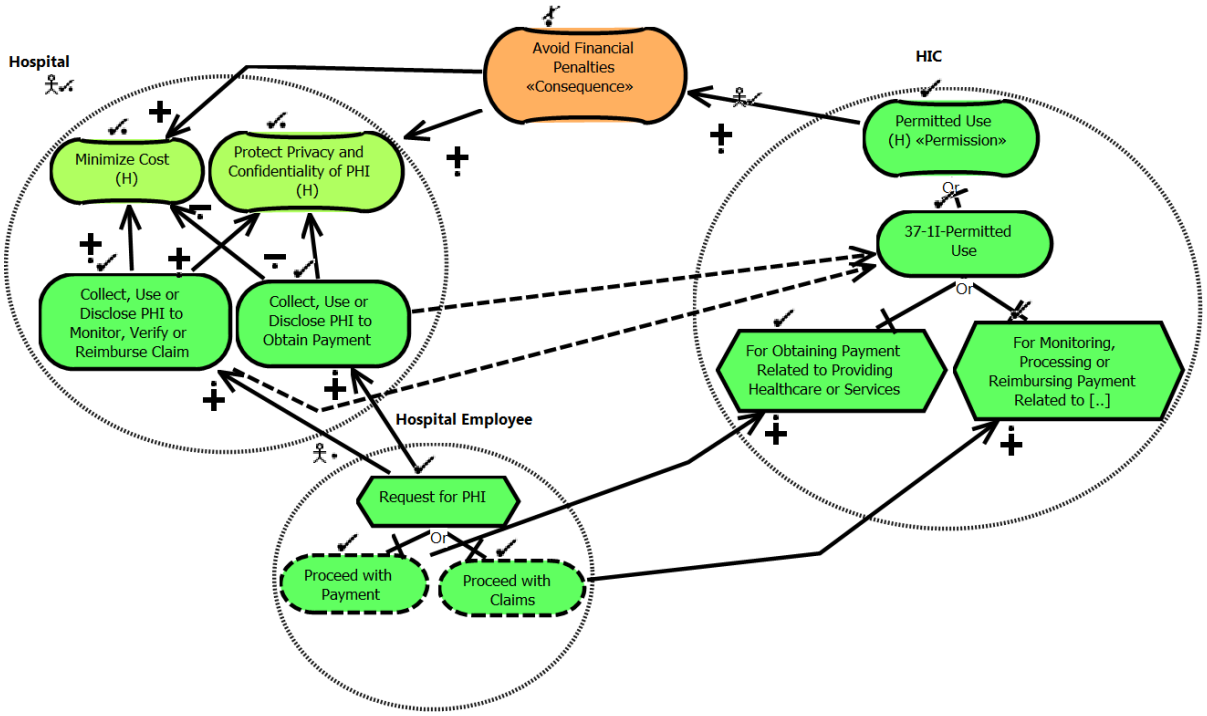

Figure D.24: Qualitative Analysis – Proceed a Payment

Qualitative Analysis of Disclose PHI to Hospital for Breach

Figure D.25 and Figure D.26 present the qualitative analysis (base strategy) for disclosing PHI for payment.

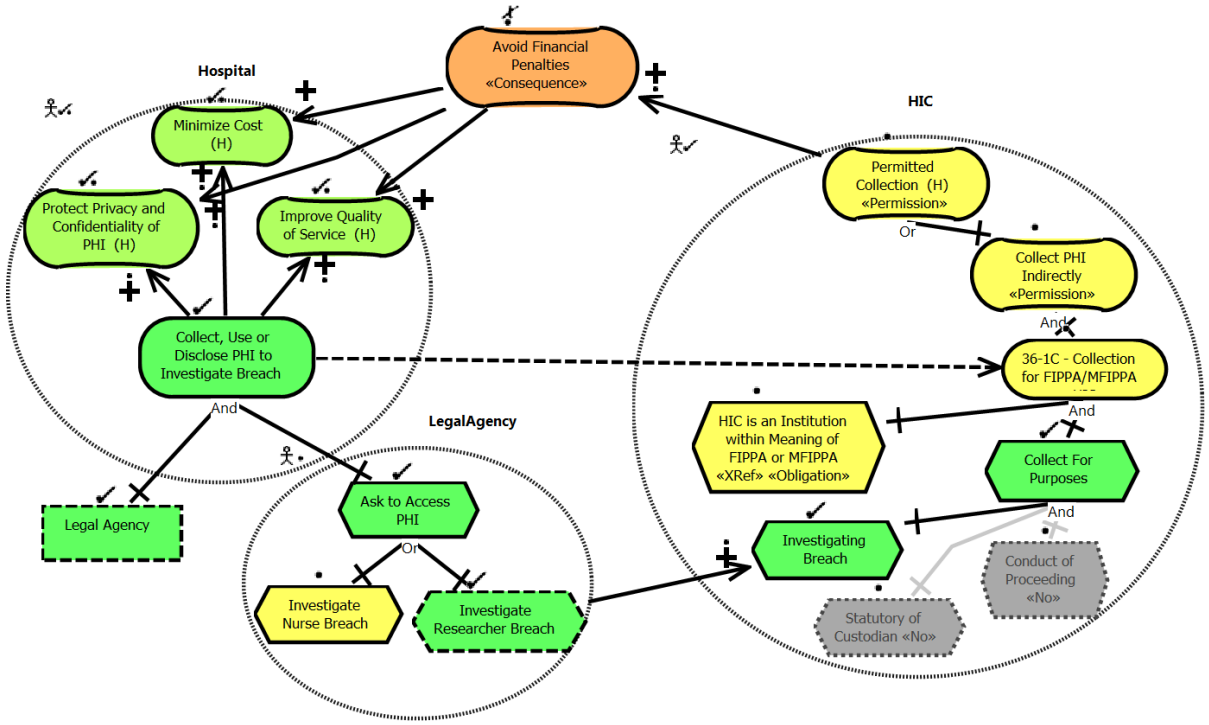

Figure D.25: Qualitative Analysis – Investigating Breach (1)

Qualitative Analysis Disclose PHI to Researchers

Figure D.27, Figure D.28, Figure D.29 and Figure D.30 present the qualitative analysis (base strategy) for disclosing PHI to researchers.

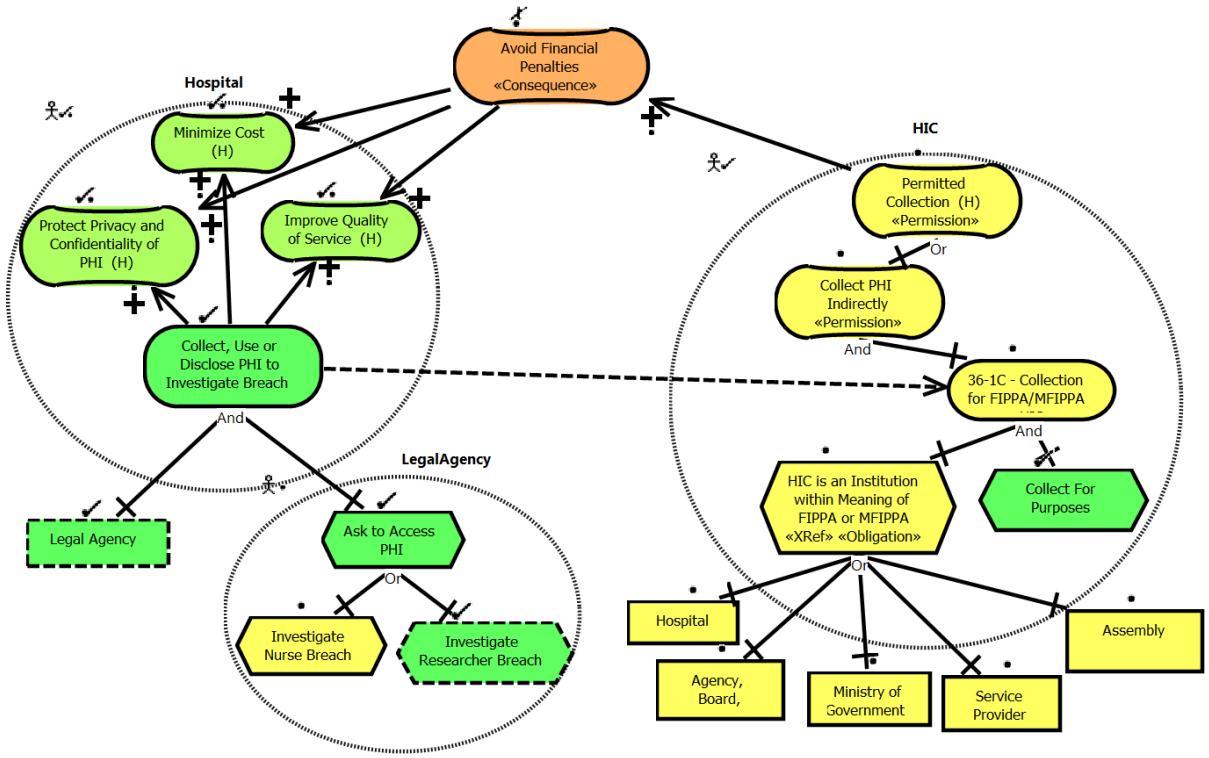

Figure D.26: Qualitative Analysis – Investigating Breach (2)

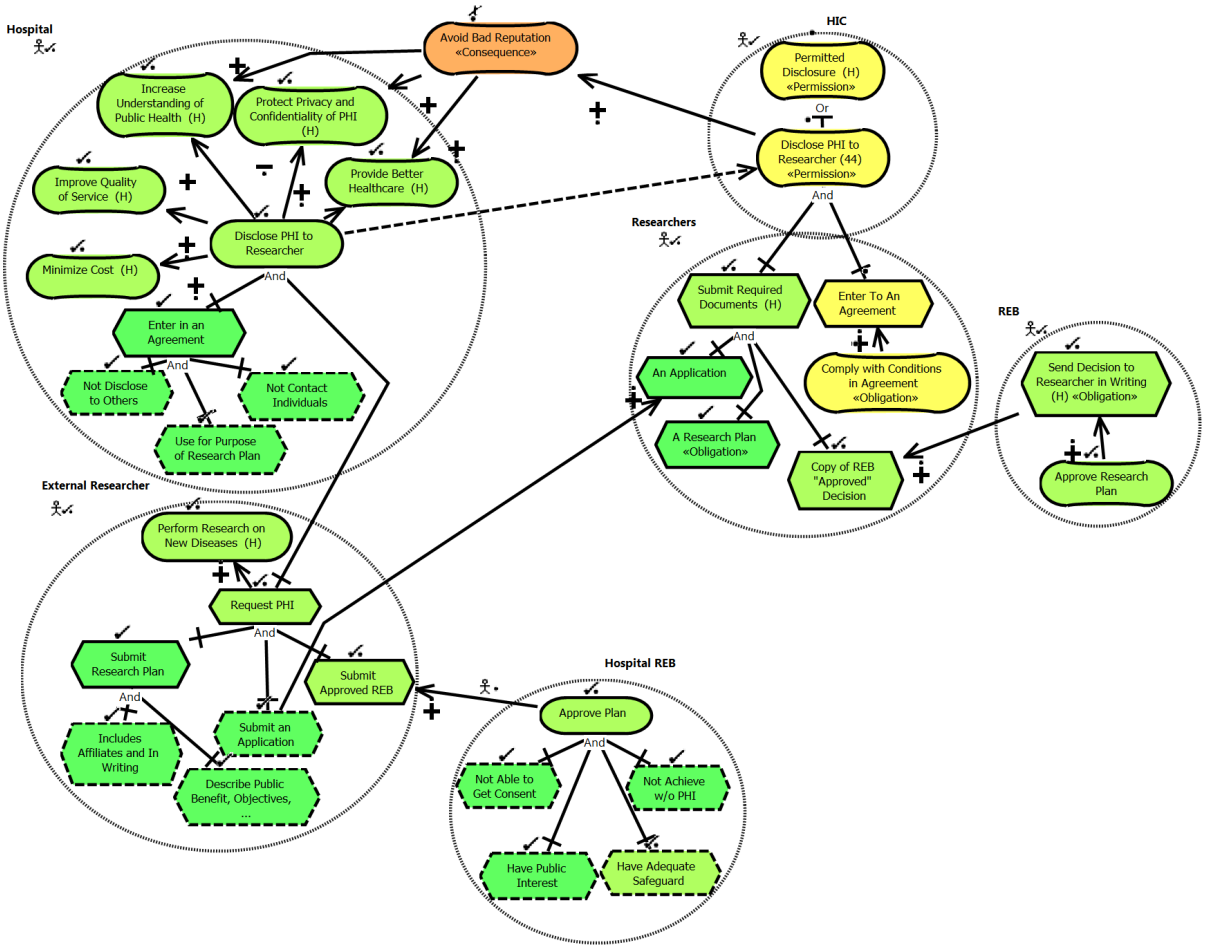

Figure D.27: Qualitative Analysis – Disclose to Researchers (1)

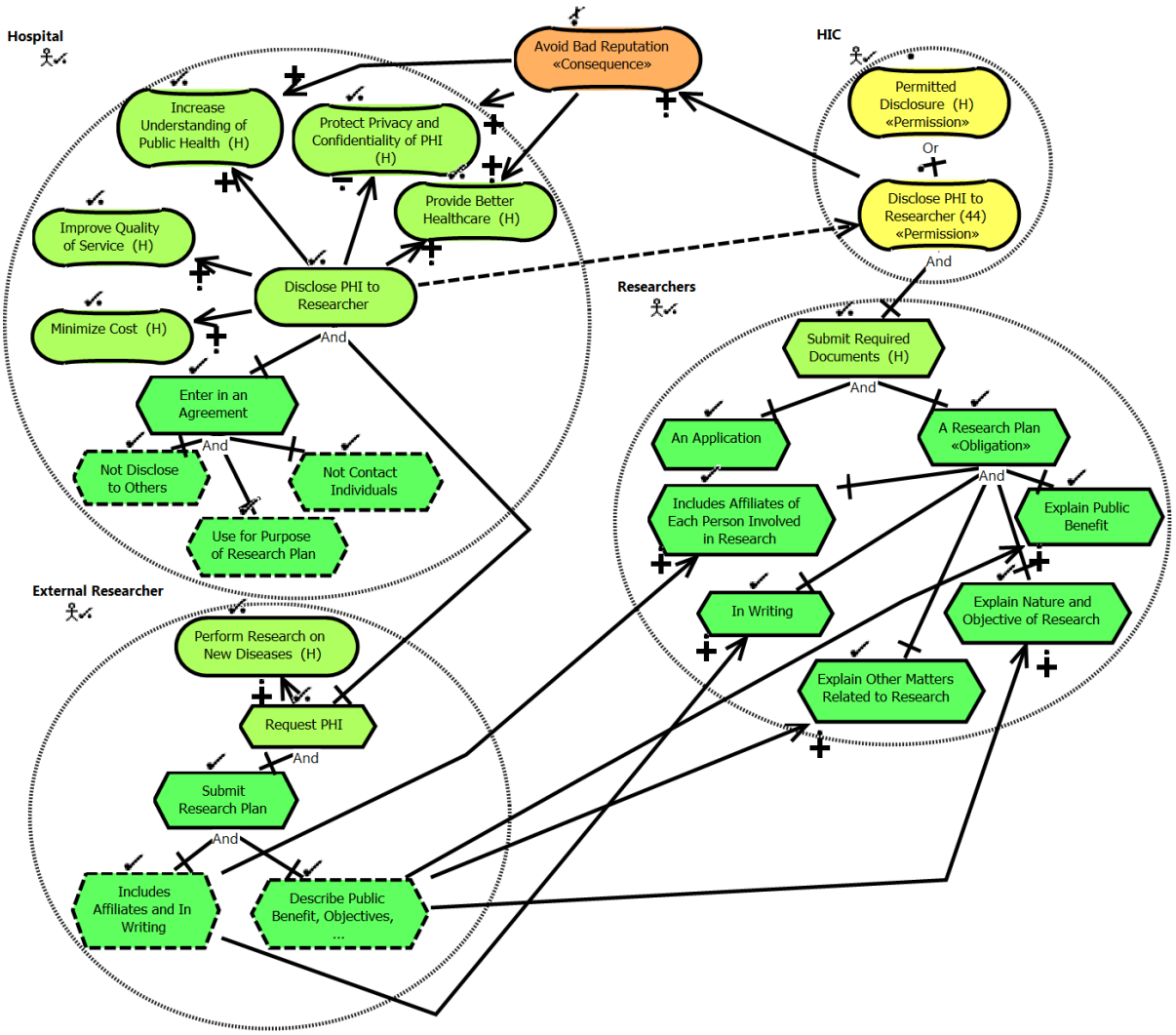

Figure D.28: Qualitative Analysis – Disclose to Researchers (2)

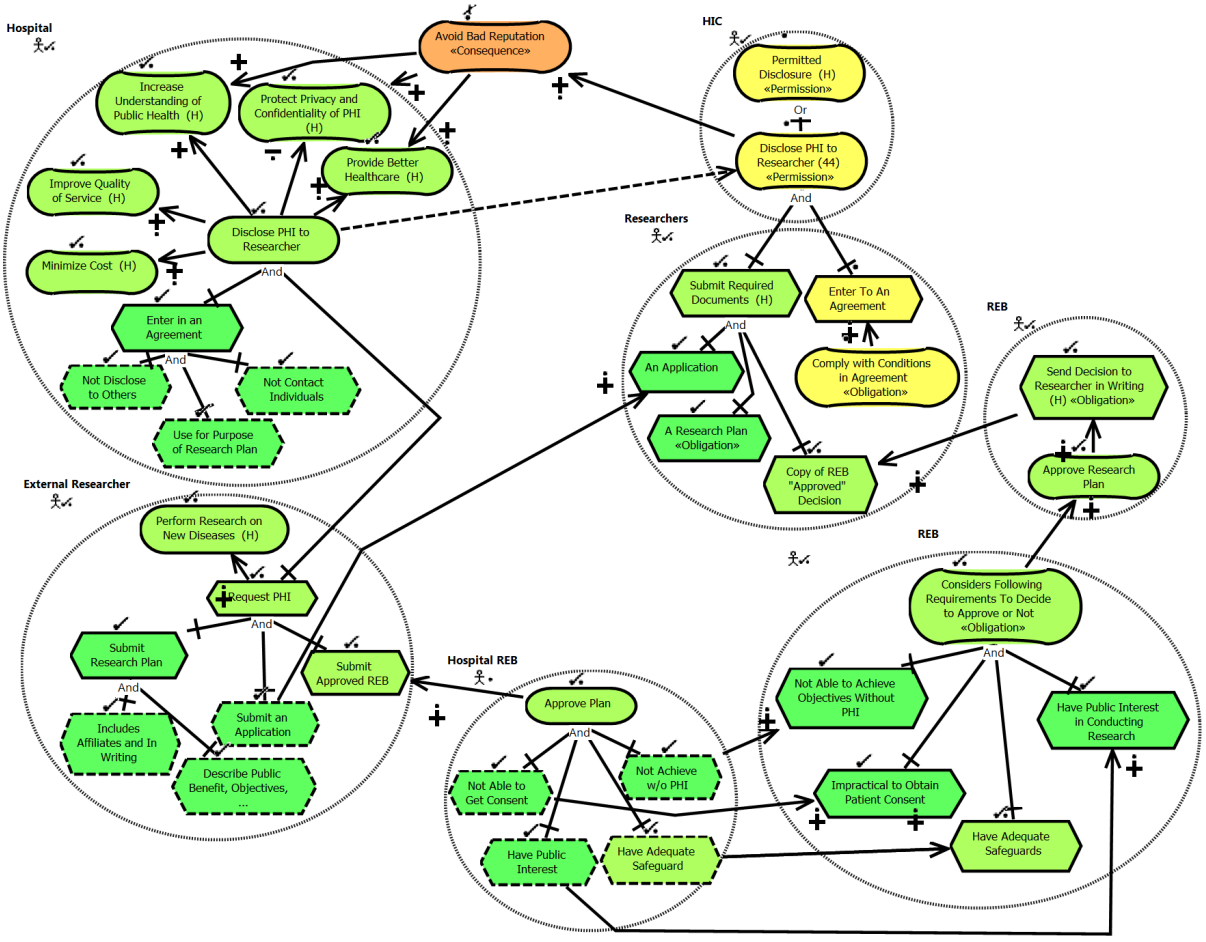

Figure D.29: Qualitative Analysis – Disclose to Researchers (3)

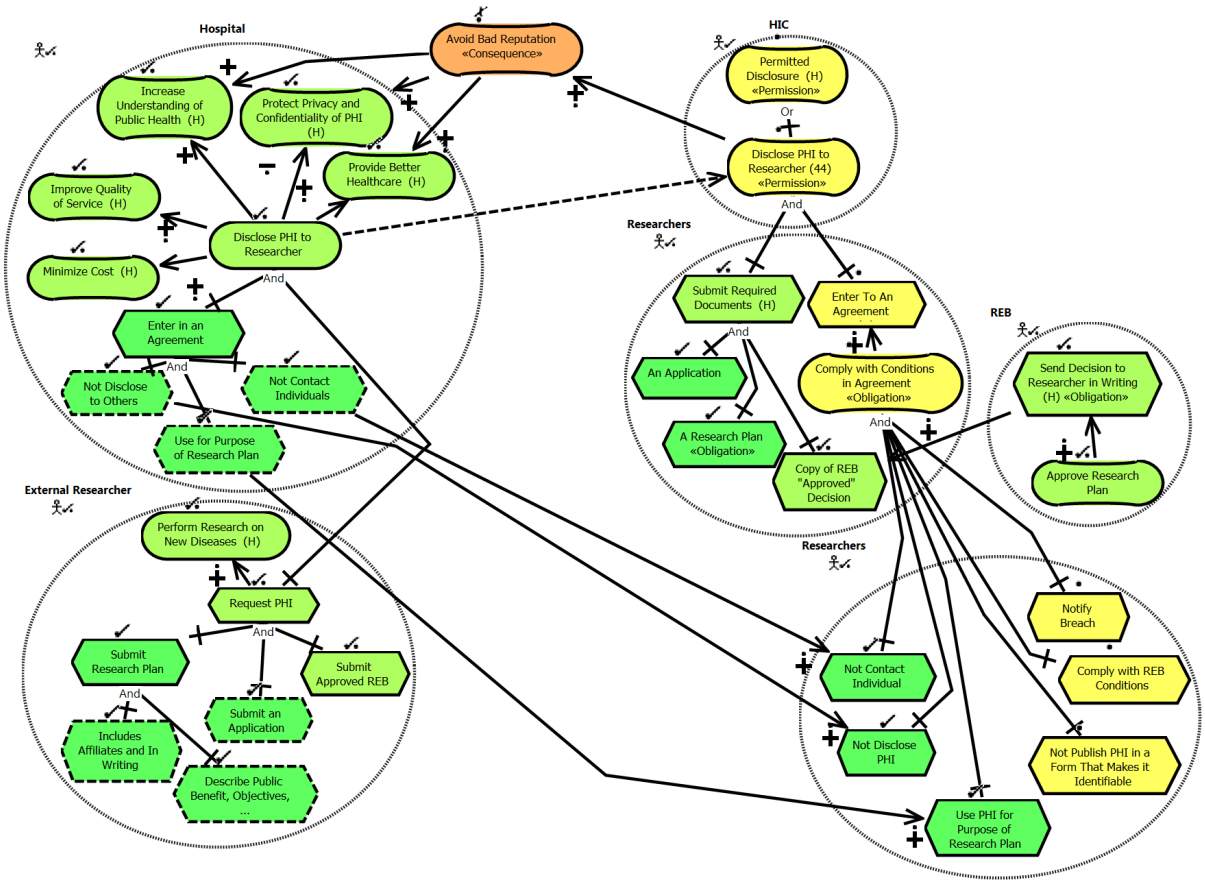

Figure D.30: Qualitative Analysis – Disclose to Researchers (4)

Appendix E

Multiple Regulation - Models

This appendix presents parts of three different regulations Quality of Care Information Protection Act, Freedom of Information and Protection of Privacy Act and with their Hohfeldian and Legal-GRL models. In addition we provide the pair-wise comparison between these regulations and parts of PHIPA.

E.1 Quality of Care Information Protection Act, 2004 (QoCIPA)

Disclosure to quality of care committee

3. Despite this Act and PHIPA, a person **may** disclose any information to a quality of care committee for the purposes of the committee. → Privilege-NoClaim Statement → Permission Goal.

Table E.1 summarizes the statement's parts and Figure E.1 shows the statement modeled in Legal GRL.

Table E.1: QoCIPA - Statement 3

XRef	Despite PHIPA
Actor	A Person
Modal Verb	May
Clause	Disclose any information to a quality of care committee for the purposes of the committee.

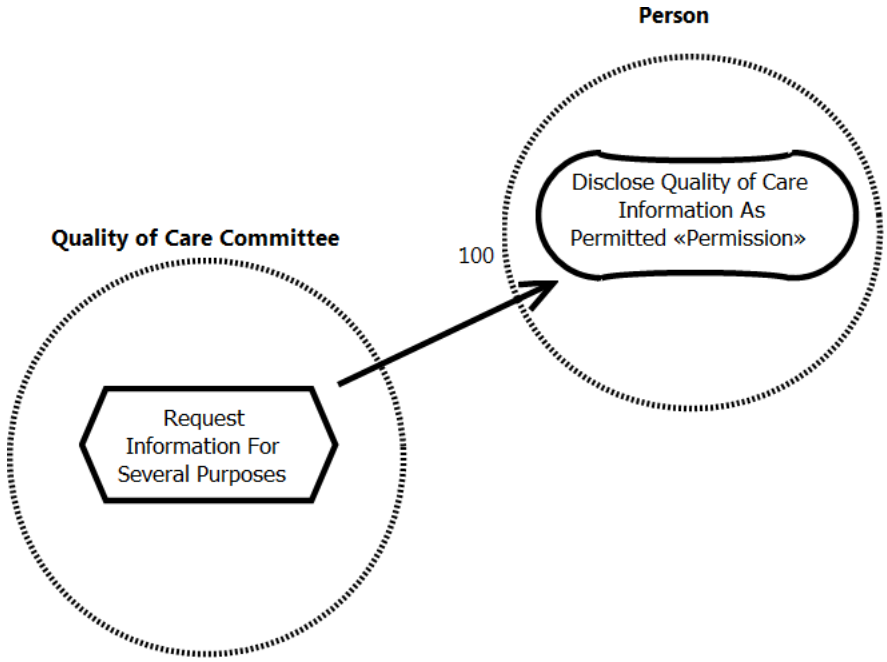

Figure E.1: Article 3 - Disclosure to Quality of Care

Quality of care information

4. (1) Despite PHIPA no person **shall** disclose quality of care information except as permitted by this Act. → Duty-Claim Statement → Obligation Goal.

Table E.2 summarizes the statement's parts and Figure E.2 shows the statement modeled in Legal GRL.

Exception, quality of care committee

(3) Despite subsection (1) and PHIPA, a quality of care committee **may** disclose quality of care information to: → Privilege-NoClaim Statement → Permission Goal.

Table E.2: QCIPA - Statement 4(1)

XRef	Despite PHIPA
Actor	A Person
Modal Verb	Shall not
Clause	Disclose quality of care information
Exception	Permitted by this act - 3

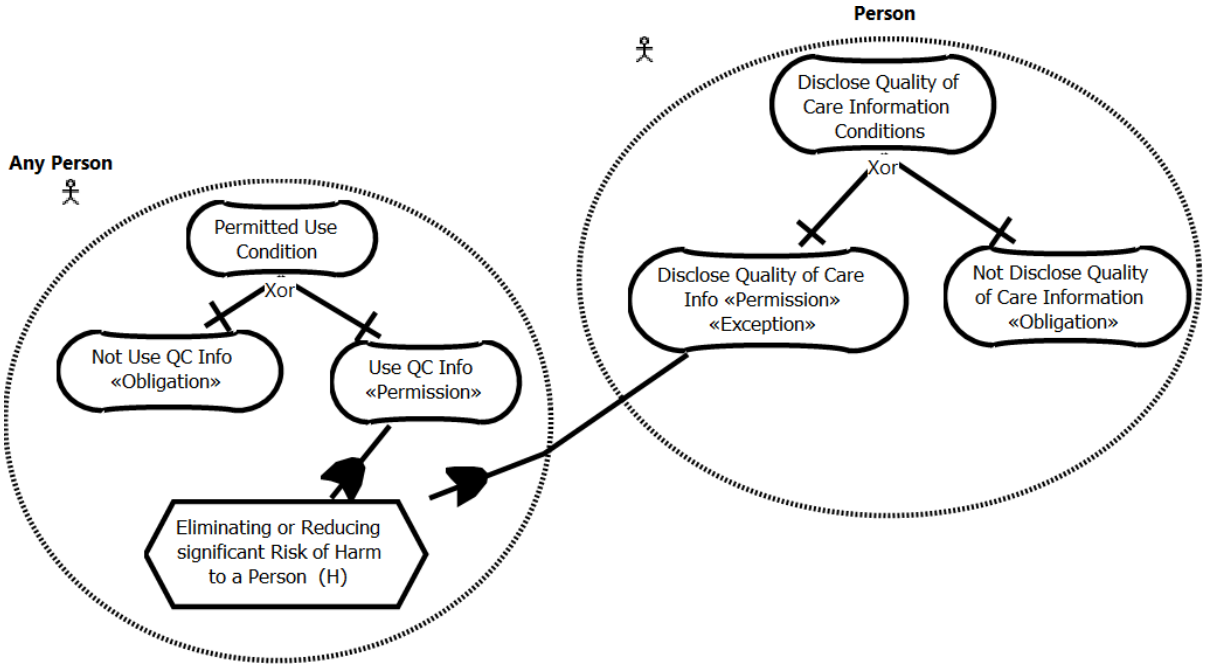

Figure E.2: Quality of Care Information - Statement 4(1)(4)(5)

Table E.3 summarizes the statement's parts and Figure E.3 shows the statement modeled in Legal GRL.

Table E.3: QoCIPA - Statement 4(3)

XRef	Despite PHIPA
Actor	A quality of care committee
Modal Verb	May
Clause	Disclose Quality of care information to a or b

(a) the management of the health facility or entity mentioned in sub-clause (a) (ii) of the definition of "quality of care committee" in section 1 that established, appointed or

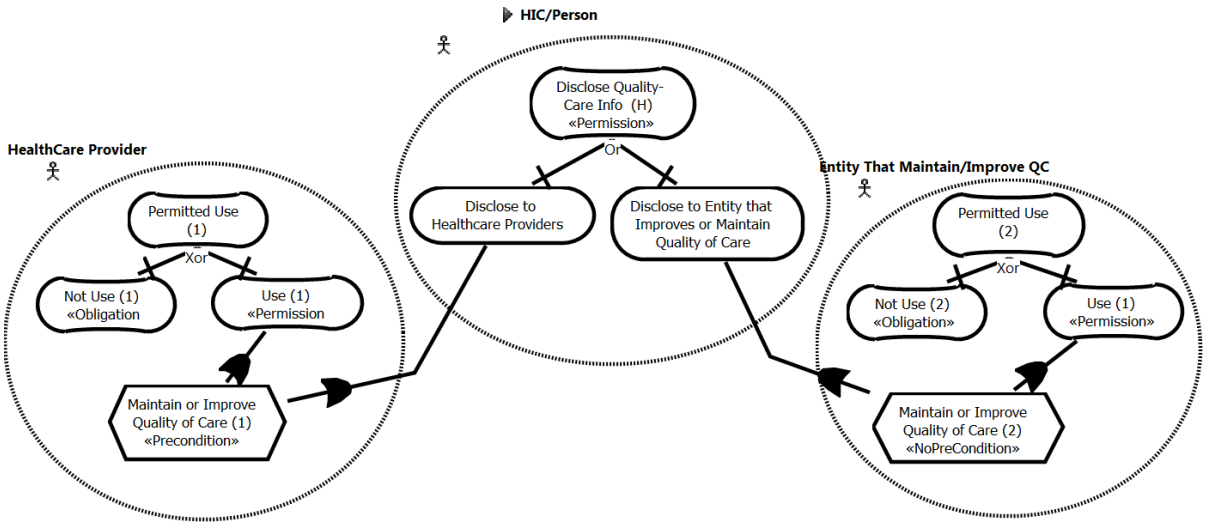

Figure E.3: Quality of Care Information - Statement 4(3)(5)

approved the committee **if** the committee considers it appropriate to do so for the purpose of improving or maintaining the quality of health care provided in or by the facility or entity; or health facility or entity mentioned in sub-clause (a) (ii) of the definition of "quality of care committee": by an entity that is prescribed by the regulations and that provides health care, or

precondition: if the committee [...] purpose of improving or maintaining [...].

(b) the management of a health facility or health care provider, where an entity mentioned in subclause (a) (iii) of the definition of "quality of care committee" in section 1 carries on activities for the purpose of improving or maintaining the quality of health care provided by the facility, the provider or a class including the facility or the provider, **if** the committee considers it appropriate to do so for the purpose of improving or maintaining the quality of health care provided in or by the facility, provider or class.

A health facility [...] in subclause (a) (iii) of the definition of "quality of care committee" in section 1: (iii) by an entity that is prescribed by the regulations and that carries on activities for the purpose of improving or maintaining the quality of care provided by a health facility, a health care provider or a class of health facility or health care provider.

precondition: if the committee [...] purpose of improving or maintaining [...].

Exception, any person

(4) Despite subsection (1) and PHIPA, a person **may** disclose quality of care information **if** the disclosure is necessary for the purposes of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. → Privilege-NoClaim Statement → Permission Goal.

Table E.4 summarizes the statement's parts and Figure E.2 shows the statement modeled in Legal GRL.

Table E.4: QoCIPA - Statement 4(4)

XRef	Despite PHIPA
Actor	A person
Modal Verb	May
Clause	Disclose quality of care information
Precondition	if the disclosure is necessary for [...]

Use of information

(5) A person to whom information is disclosed under subsection (3), (4) or (6) **shall not** use the information **except** for the purposes for which the information was disclosed to the person. → Duty-Claim Statement → Obligation Goal.

Table E.5 summarizes the statement's parts and Figure E.3 shows the statement modeled in Legal GRL.

Table E.5: QoCIPA - Statement 4(5)

Actor	A person to [...]
Modal Verb	Shall not
Clause	Use the information
Exception	For purposes for which the information was disclosed to the person

(6) A member of the management of a health facility or entity described in subsection (3) to whom quality of care information is disclosed under that subsection **may** disclose the information to an agent or employee of the facility or entity **if** the disclosure is necessary for the purposes of improving or maintaining the quality of health care provided in or by the facility or entity. → Privilege-NoClaim Statement → Permission Goal.

Table E.6 summarizes the statement's parts and Figure E.4 shows the statement modeled in Legal GRL.

Table E.6: QoCIPA - Statement 4(6)

Actor	A member of the management of a health facility or entity described [...]
Modal Verb	May
Clause	Disclose the information to an agent or [...]
Precondition	If the disclosure is necessary for [...]

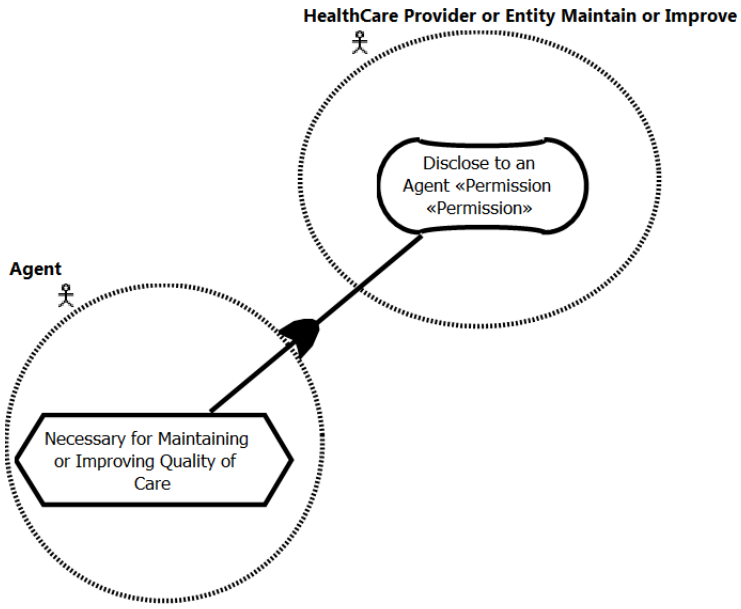

Figure E.4: Quality of Care Information - Statement 4(6)

E.2 Freedom of Information and Protection of Privacy Act, 2011 (FIPPA)

Collection of personal information

38. (2) No person **shall** collect personal information on behalf of an institution **unless** the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. → Duty-Claim Statement → Obligation Goal.

Table E.7 summarizes the statement's parts and Figure E.5 shows the statement modeled in Legal GRL.

Table E.7: FIPPA - Statement 38 (2)

Actor	A person
Modal Verb	Shall not
Clause	Collect personal information on behalf of an institution
Exception	The collection is expressly authorized by statute, used for the purposes [...]

Manner of collection

39. (1) Personal information **shall** only be collected by an institution directly from the individual to whom the information relates unless, → Duty-Claim Statement → Obligation Goal.

(a) the individual authorizes another manner of collection;

(b) the personal information may be disclosed to the institution concerned under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act;

(c) the Commissioner has authorized the manner of collection under clause 59 (c);

(d) the information is in a report from a reporting agency in accordance with the Consumer Reporting Act;

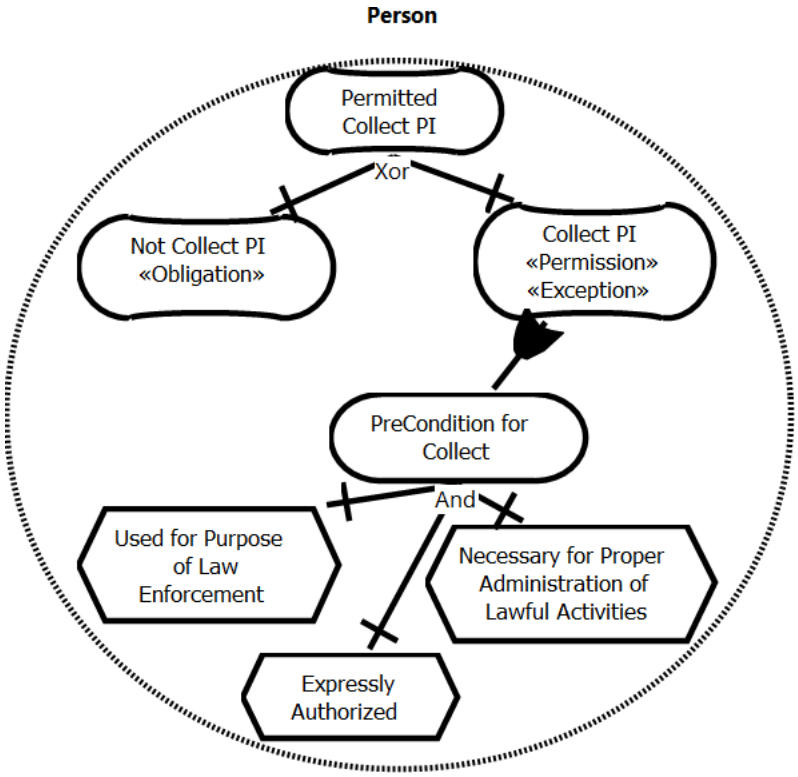

Figure E.5: FIPPA - Statement 38

(e) the information is collected for the purpose of determining suitability for an honor or award to recognize outstanding achievement or distinguished service;

(f) the information is collected for the purpose of the conduct of a proceeding or a possible proceeding before a court or tribunal;

(g) the information is collected for the purpose of law enforcement; or

(h) another manner of collection is authorized by or under a statute.

Table E.8 summarizes the statement's parts and Figure E.6 shows the statement modeled in Legal GRL.

Notice to individual

(2) Where personal information is collected on behalf of an institution, the head **shall**, unless notice is waived by the responsible minister, inform the individual to whom the information relates of: → Duty-Claim Statement → Obligation Goal.

Table E.8: FIPPA - Statement 39 (1)

Actor	An institution
Modal Verb	Shall
Clause	Collect Personal information directly from the individual to whom the information relates
Exception	Statements (a) to (h)

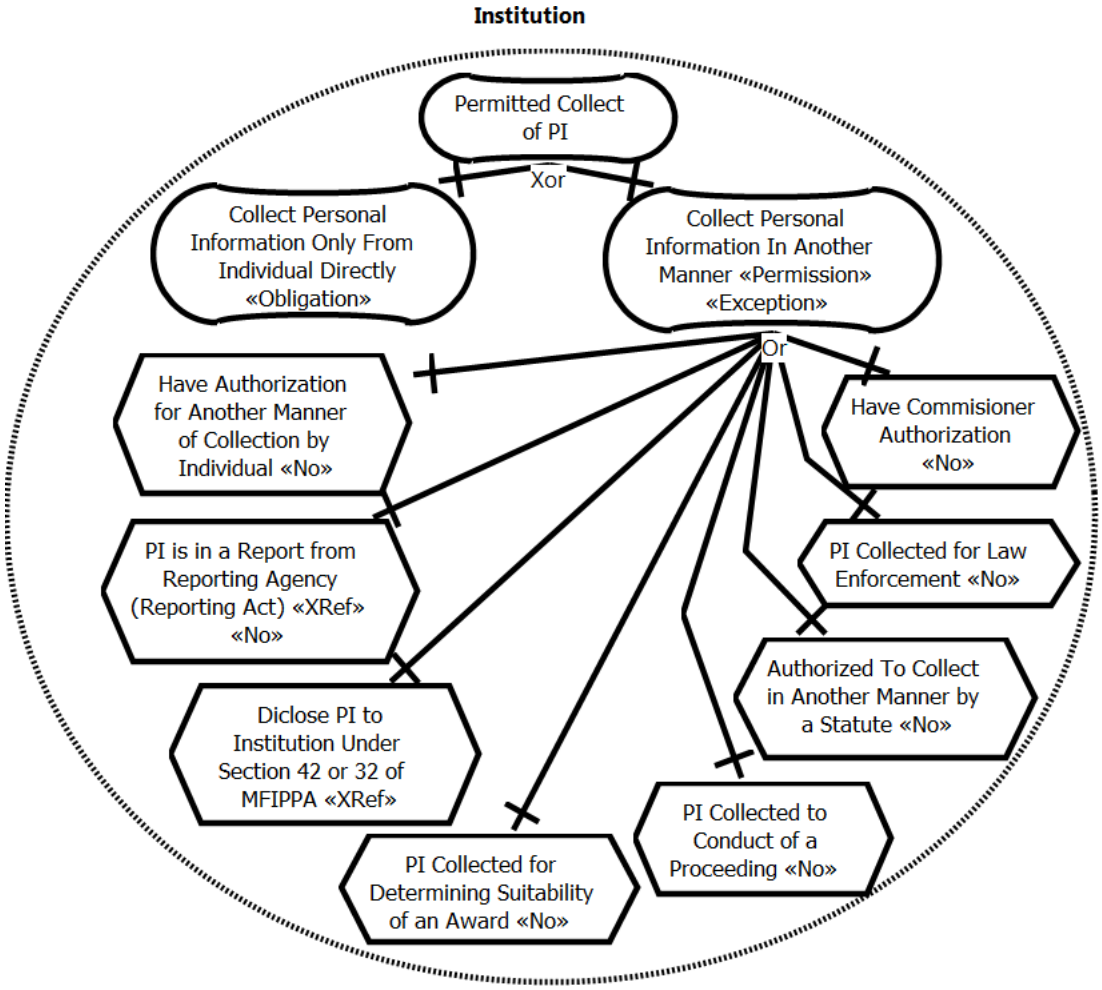

Figure E.6: FIPPA - Statement 39(1)

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who

can answer the individual's questions about the collection.

Table E.9 summarizes the statement's parts and Figure E.7 shows the statement modeled in Legal GRL.

Table E.9: FIPPA - Statement 39 (2)

Precondition	Where personal information is collected on behalf of an institution
Actor	Head of institution
Modal Verb	Shall
Clause	Inform individual [...] (a),(b) and (c)
Exception	notice is waived

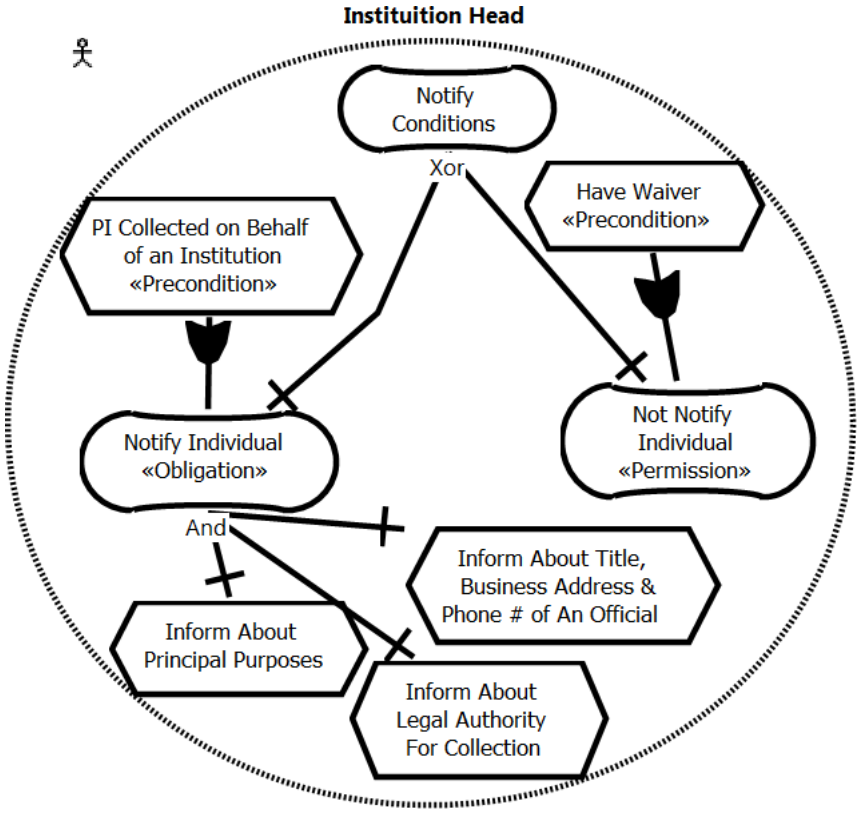

Figure E.7: FIPPA - Statement 39(2)

Use of personal information

41.(1) An institution **shall not** use personal information in its custody or under its control except, → Duty-Claim Statement → Obligation Goal.

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose;

(c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act; or

(d) subject to subsection (2), an educational institution may use personal information in its alumni records and a hospital may use personal information in its records for the purpose of its own fundraising activities, if the personal information is reasonably necessary for the fundraising activities.

Table E.10 summarizes the statement's parts and Figure E.8 shows the statement modeled in Legal GRL.

Table E.10: FIPPA - Statement 41 (1)

Actor	An institution
Modal Verb	Shall not
Clause	Use personal information [...]
Exception	Statements (a) to (d)

Notice on using personal information for fundraising

(2) In order for an educational institution to use personal information in its alumni records or for a hospital to use personal information in its records, either for its own fundraising activities or for the fundraising activities of an associated foundation, the educational institution or hospital **shall**: → Duty-Claim Statement → Obligation Goal.

(a) give notice to the individual to whom the personal information relates when the

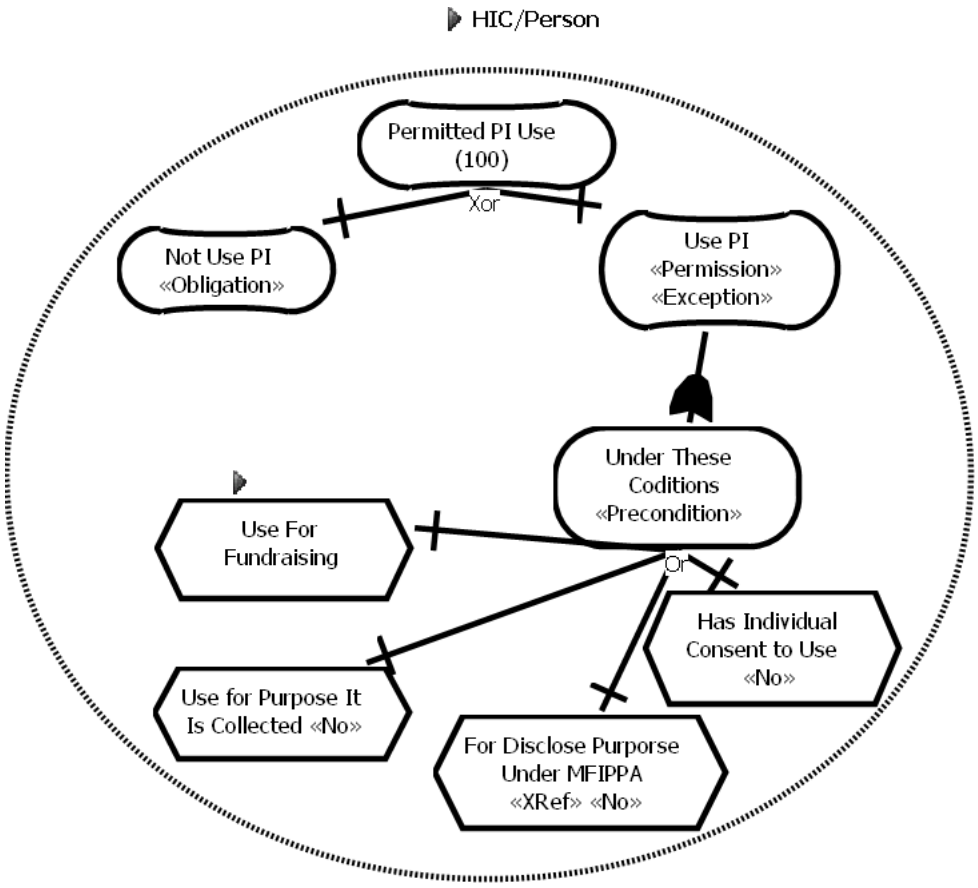

Figure E.8: FIPPA - Statement 41(1)

individual is first contacted for the purpose of soliciting funds for fundraising of his or her right to request that the information cease to be used for fundraising purposes;

(b) periodically and in the course of soliciting funds for fundraising, give notice to the individual to whom the personal information relates of his or her right to request that the information cease to be used for fundraising purposes; and

(c) periodically and in a manner that is likely to come to the attention of individuals who may be solicited for fundraising, publish a notice of the individual's right to request that the individual's personal information cease to be used for fundraising purposes.

Table E.11 summarizes the statement's parts and Figure E.9 shows the statement modeled in Legal GRL.

Table E.11: FIPPA - Statement 41 (2)

Precondition	In order for an educational [...] to use [...]
Actor	The educational institution or hospital
Modal Verb	Shall
Statement a	Give notice to the individual to whom the personal information relates [...]
Precondition a	When the individual [...]
Statement b	Give notice to the individual to whom the personal information relates [...]
Precondition b	Periodically and in the course of soliciting funds for fundraising
Clause c	Publish to the individual to whom the personal information relates [...]
Precondition c	Periodically and in a manner that is likely to come to the attention of individuals

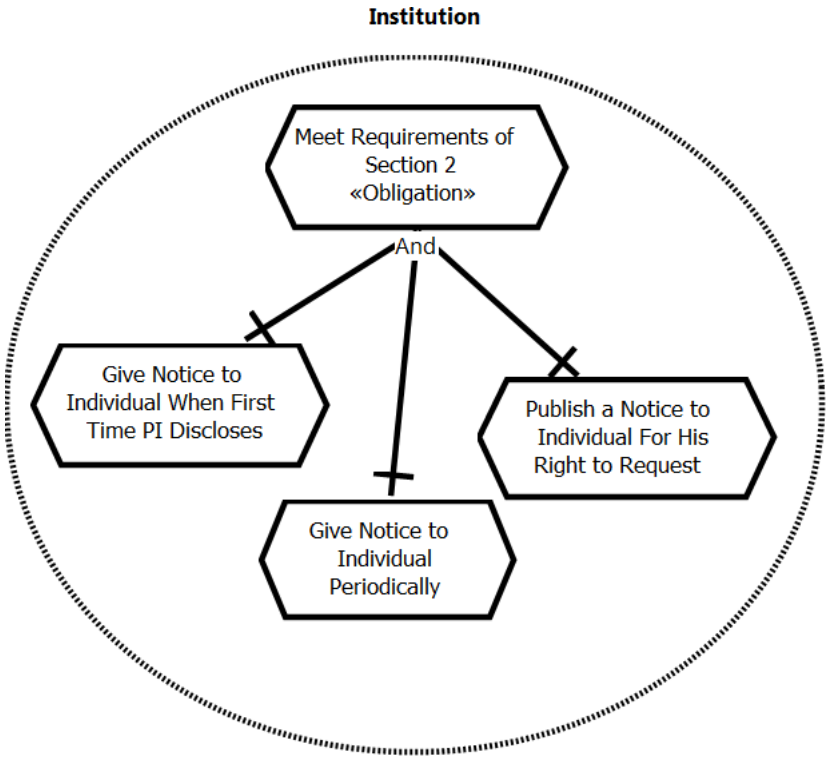

Figure E.9: FIPPA - Statement 41 (2)

Where disclosure permitted

42. (1) An institution **shall not** disclose personal information in its custody or under its control **except**, → Duty-Claim Statement → Obligation Goal.

(o) subject to subsection (2), an educational institution may disclose personal information in its alumni records, and a hospital may disclose personal information in its records, for the purpose of its own fundraising activities or the fundraising activities of an associated foundation if,

(i) the educational institution and the person to whom the information is disclosed, or the hospital and the person to whom the information is disclosed, have entered into a written agreement that satisfies the requirements of subsection (3), and (ii) the personal information is reasonably necessary for the fundraising activities.

Table E.12 summarizes the statement's parts and Figure E.10 shows the statement modeled in Legal GRL.

Table E.12: FIPPA - Statement 42 (1)

Actor	An institution
Modal Verb	Shall not
Clause	Disclose personal information [...]
Exception	Statements (a) to (o)

Notice on disclosing personal information for fundraising

(2) In order for an educational institution to disclose personal information in its alumni records or for a hospital to disclose personal information in its records, either for the purpose of its own fundraising activities or the fundraising activities of an associated foundation, the educational institution or hospital **shall** ensure that: → Duty-Claim Statement → Obligation Goal.

(a) notice is given to the individual to whom the personal information relates when the individual is first contacted for the purpose of soliciting funds for fundraising of his or her right to request that the information cease to be disclosed for fundraising purposes;

(b) periodically and in the course of soliciting funds for fundraising, notice is given to the individual to whom the personal information relates of his or her right to request that the information cease to be disclosed for fundraising purposes; and

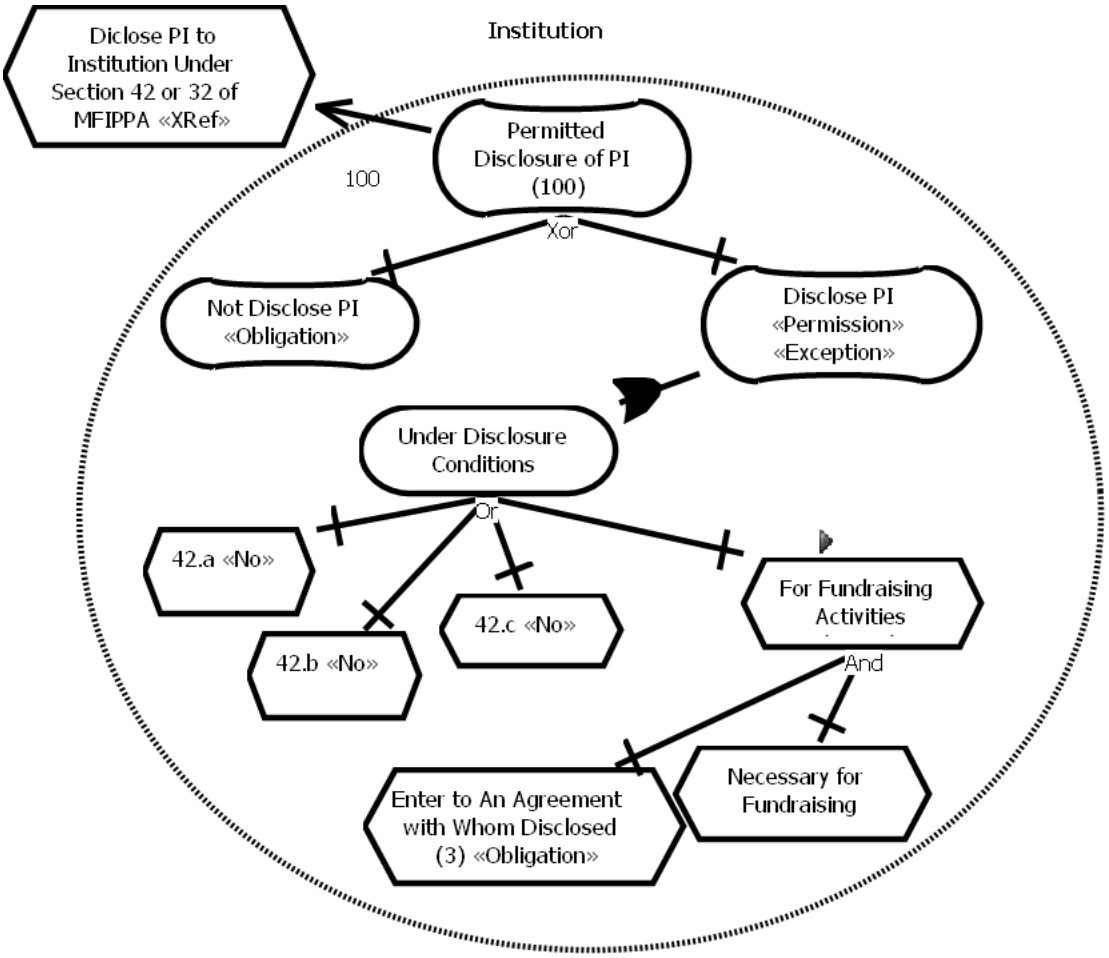

Figure E.10: FIPPA - Statement 42 (1)

(c) periodically and in a manner that is likely to come to the attention of individuals who may be solicited for fundraising, notice is published in respect of the individual's right to request that the individual's personal information cease to be disclosed for fundraising purposes.

Table E.13 summarizes the statement's parts and Figure E.11 shows the statement modeled in Legal GRL.

Table E.13: FIPPA - Statement 42 (2)

Precondition	In order for an educational [...] to disclose [...]
Actor	The educational institution or hospital
Modal Verb	Shall
Clause a	Give notice to the individual to whom the personal information relates [...]
Precondition a	When the individual [...]
Clause b	Give notice to the individual to whom the personal information relates [...]
Precondition b	Periodically and in the course of soliciting funds for fundraising
Clause c	Publish to the individual to whom the personal information relates [...]
Precondition c	Periodically and in a manner that is likely to come to the attention of individuals

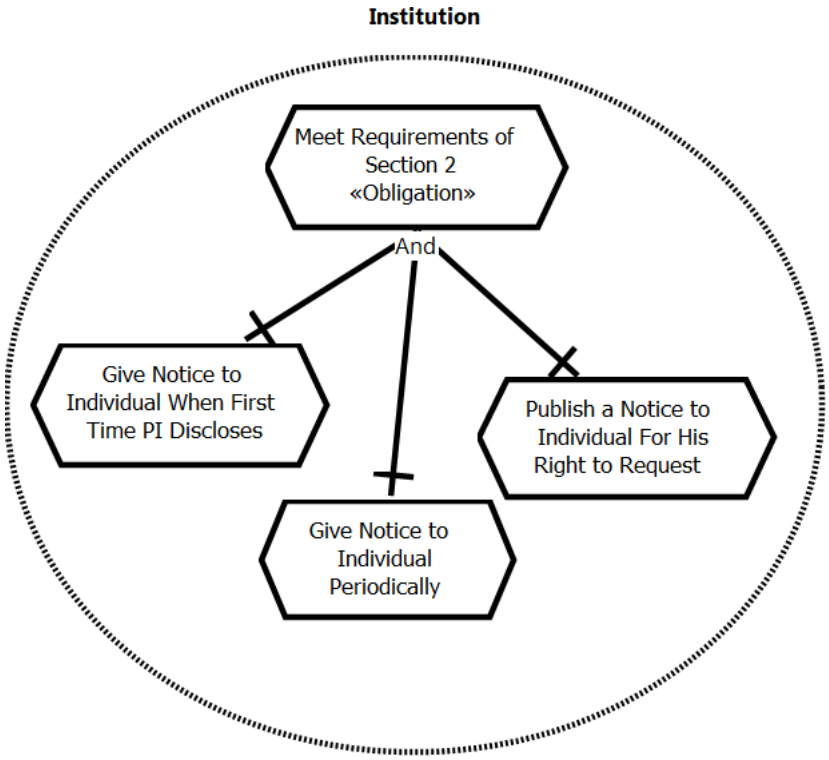

Figure E.11: FIPPA - Statement 42 (2)

Fundraising agreement

(3) An agreement between an educational institution and another person for the disclosure of personal information in the educational institution's alumni records for fundrais-

ing activities, or an agreement between a hospital and another person for the disclosure of personal information in the hospital's records for fundraising activities, **must**: → Duty-Claim Statement → Obligation Goal.

(a) require that the notice requirements in subsection (2) are met;

(b) require that the personal information disclosed under clause (1) (o) be disclosed to the individual to whom the information relates upon his or her request; and

(c) require that the person to whom the information is disclosed **shall** cease to use the personal information of any individual who requests that the information not be used.

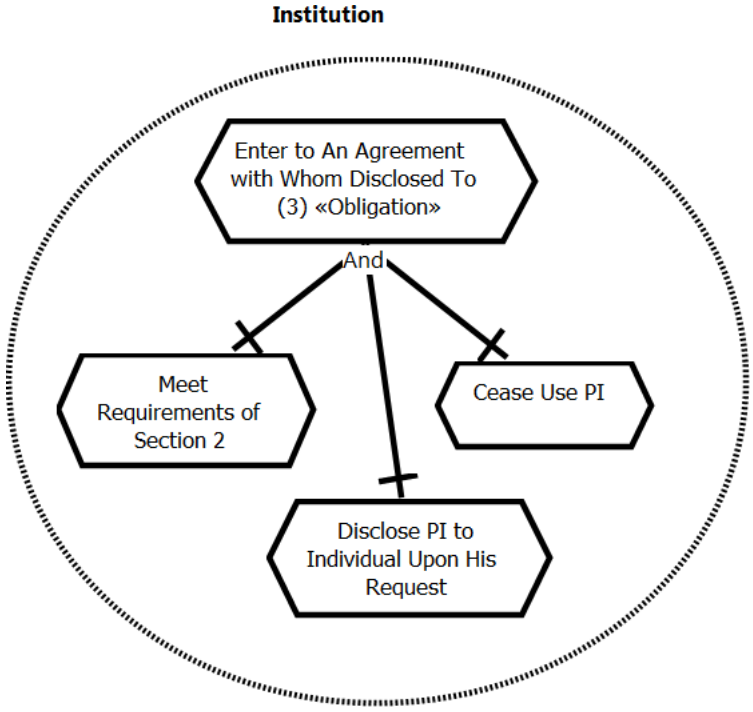

Figure E.12: FIPPA - Statement 42 (3)

E.3 Health Care Consent Act, 1996 (HCCA)

Consent To Treatment – No treatment without consent

10. (1) A health practitioner who proposes a treatment for a person **shall not** administer the treatment, and **shall** take reasonable steps to ensure that it is not administered, **unless**: → Duty-Claim Statement → Obligation Goal.

(a) he or she is of the opinion that the person is capable with respect to the treatment, and the person has given consent; or

(b) he or she is of the opinion that the person is incapable with respect to the treatment, and the person's substitute decision-maker has given consent on the person's behalf in accordance with this Act.

Table E.14 summarizes the statement's parts and Figure E.13 shows the statement modeled in Legal GRL.

Table E.14: HCCA - Statement 10(1)

Actor	A health practitioner
Modal Verb	Shall not
Clause 1	Administer treatment
Modal Verb	Shall
Clause 2	Take reasonable steps to ensure that it is not administered
Exception	Statements (a) to (b)

Elements of consent

11. (1) The following are the elements required for consent to treatment: → Duty-Claim Statement → Obligation Goal.

1. The consent **must** relate to the treatment.
2. The consent **must** be informed.
3. The consent **must** be given voluntarily.
4. The consent **must** not be obtained through misrepresentation or fraud.

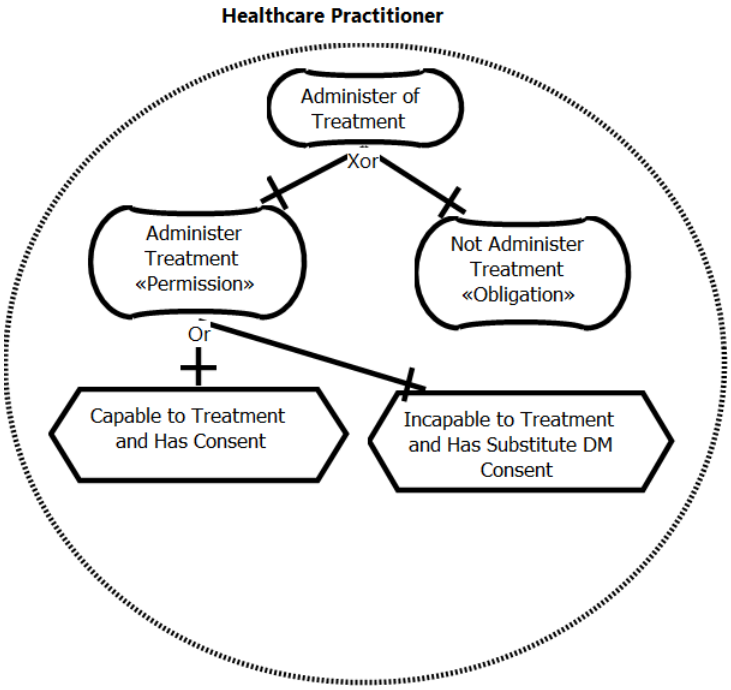

Figure E.13: HCCA - Statement 10(1)

Table E.15 summarizes the statement's parts and Figure E.14 shows the statement modeled in Legal GRL.

Table E.15: HCCA - Statement 11(1)

Actor	A consent to treatment
Modal Verb	Must
Clause 1	Relate to the treatment,
Clause 2	Be informed,
Clause 3	Be given voluntarily, and
Clause 4	Not be obtained through misrepresentation or fraud.

Express or implied

(4) Consent to treatment **may** be express or implied. → Privilege-NoClaim Statement → Permission Goal (see Table E.16).

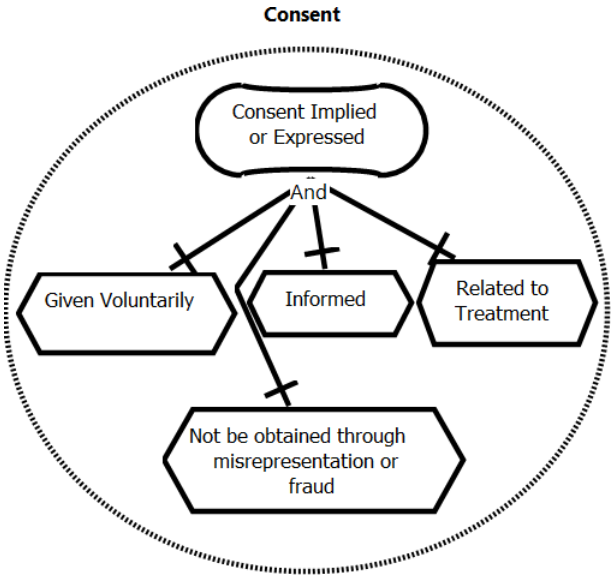

Figure E.14: HCCA - Statement 11(1)(4)

Table E.16: HCCA - Statement 11(4)

Actor	A consent to treatment
Modal Verb	May
Clause	Be expressed or implied

E.4 Personal Health Information Protection Act, 2004 (PHIPA)

Fundraising

32. (1) Subject to subsection (2), an HIC **may** collect, use or disclose PHI about an individual for the purpose of fundraising activities only where,

(a) the individual expressly consents; or

(b) the individual consents by way of an implied consent and the information consists only of the individual's name and the prescribed types of contact information.

Table E.17 summarizes the statement's parts and Figure E.15 shows the statement modeled in Legal GRL.

Table E.17: PHIPA - Statement 32

Actor	An HIC
Modal Verb	May
Clause 1	Administer treatment
Modal Verb	Shall
Clause 2	Collect, use or disclose PHI about an individual for the purpose of fundraising activities
Precondition	a or b
Exception	-

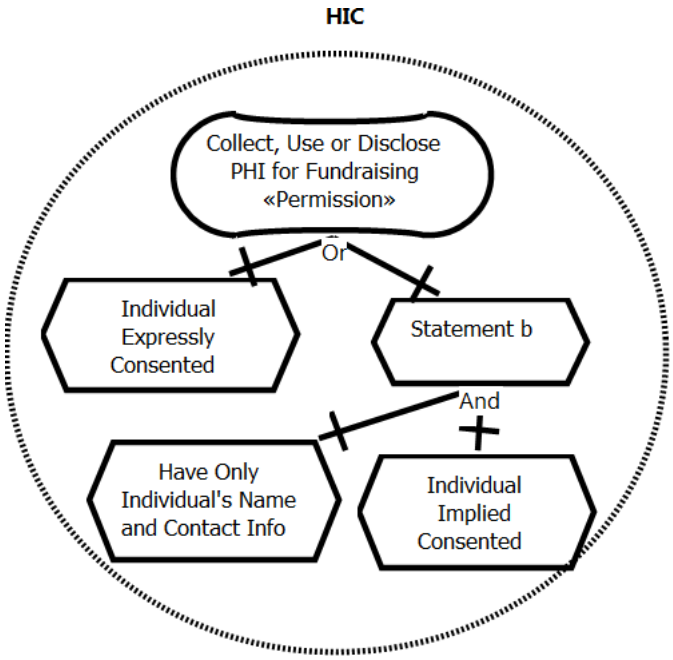

Figure E.15: PHIPA - Article 32 (1)

E.5 Pair-Wise Comparison of PHIPA with QoCIPA

In this section, we compare Articles 10 (Information practices), 11 (Accuracy), 12 (Security), 18 (Elements of consent), 29 (Requirement for consent), 31 (Use and disclosure of personal health information), 32 (Disclose for fundraising), parts of 36 (Indirect collection) (statements 1a-d), parts of 37 (Permitted Use) (statements 1a,1d, 1i and 3), 38 (Disclosures related to providing health care) (statements 1), and parts of 44 (Disclosure for research)(statements 1-6) from PHIPA with Articles 3 (Disclosure to quality of care

committee) and 4 (Quality of care information) from QoCIPA.

During the manual matching of sections between the two regulations, we identify that Articles 3 and 4 of QoCIPA do not have anything in common with Articles 10, 11, 12, 18, 32, 36 of PHIPA. We hence can limit the pair-wise comparison to Article 3 and 4 of QoCIPA and Articles 29, 31, 37, 38(1) and 44(1)-(6) of PHIPA.

In Chapter 8, we showed the pair-wise comparison results between Article 3 QoCIPA and Articles 29 and 31 of PHIPA, which are conflicts (case 6). Pair-wise comparison of Article 3 with Article 37 results in case 1 (nothing in common).

Pair-wise comparison of Article 3 with Article 38 (1) is shown in Table E.18. The result of this comparison is case 5 (subset).

Table E.18: Pair-Wise Comparison of Article 3 of QoCIPA and Article 38 (1) of PHIPA

Statement	**Statement$_1$**	**Statement$_2$**	**Comparison**
Section	Disclosure to quality of care committee	Disclosures Related to Providing Health Care	-
Actor	A person	An HIC	A person belongs to an HIC
Modal Verb	May	May	Same Modal Verb
Clause	Disclose any information to a quality of care committee for the purposes of the committee.	Disclose PHI about an individual to an HIC described in [...]	Both clauses are about disclosing information
Precondition1	-	If the disclosure is reasonably necessary for [...] and it is not reasonably possible to obtain the individual's consent in a timely manner,	
Exception 1	-	But not if the individual has expressly instructed [...]	
Clause 2	-	Disclose PHI about an individual in order for the Minister, another HIC or a local health integration network to determine or [...]	PHIPA has more clauses
Clause 3	-	Disclose PHI about an individual for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual	PHIPA has more clauses
Precondition 3	If the individual is injured, incapacitated or ill and unable to give consent personally.	PHIPA has more preconditions	
XRef	Despite PHIPA	-	

Pair-wise comparison of Article 3 with Article 44 (1) is shown in Table E.19. The result of this comparison is a case 3 while with the rest of Article 44 (2-6), there is nothing in common (case 1).

In addition:

Table E.19: Pair-Wise Comparison of Article 3 of QoCIPA and Article 44 (1) of PHIPA

Statement	**Statement$_1$**	**Statement$_2$**	**Comparison**
Section	Disclosure to quality of care committee	Disclosure for research	-
Actor	A person	An HIC	A person belongs to an HIC
Modal Verb	May	May	Same Modal Verb
Clause	Disclose Any information to a quality of care committee for the purposes of the committee.	Disclose PHI about an individual to a researcher if the researcher [...]	Both clauses are about disclosing information
(Pre)condition 1	-	Submits to the custodian [...]	additional clause or conditions in PHIPA
(Pre)condition 2	-	Enters into the agreement required by subsection	additional clause or conditions in PHIPA
XRef	Despite PHIPA	-	-

- Similar to Article 3, the comparison between Article 4 (1)(3)(4)(6) and Article 38(1) results in case 5, and in case 1 with Article 44(1).
- Pair-wise comparison of Article 4 (5) with Articles 38 and 44(1)-(6) of PHIPA illustrates case 1 as well.
- Pair-wise comparison of Article 4 (5) with Article 29 results in case 3, and in case 2 with Article 31.
- A comparison between Article 4(5) and Article 37 (1) results in a conflict (case 6) that can be resolved by following the exception.

Table E.20: Pair-Wise Comparison of Article 3 of QoCIPA and Article 37 (1) of PHIPA

Statement	**Statement$_1$**	**Statement$_2$**	**Comparison**
Section	Quality of care information	Permitted Use	-
Actor	A person	An HIC	A person belongs to an HIC
Modal Verb	Shall	May	-
Clause	Not Use the information	Use PHI about an individual for (a) - (k)	-
Exception	For purposes for which the information was disclosed to the person	-	-
Precondition	-	-	
XRef	-	-	-

E.6 Pair-Wise Comparison of PHIPA with FIPPA

In this section, we compare Articles 10 (Information practices), 11 (Accuracy), 12 (Security), 18 (Elements of consent), 29 (Requirement for consent), 31 (Use and disclosure of personal health information), 32 (Disclosure for fundraising), parts of 36 (Indirect collection) (statements 1a-d), parts of 37 (Permitted Use) (statements 1a,1d, 1i and 3), 38 (Disclosures related to providing health care) (statements 1a and 2), and parts of 44 (Disclosure for research)(statements 1-6) of PHIPA with Articles 38(2) (Collection of personal information), 39 (1)(2)(Manner of collection), 41 (Use of personal information) and 42 (Where disclosure permitted) of FIPPA.

In the first pass, based on the step for finding the matching sections of the two regulations, we identify that Articles 41 and 42 of FIPPA are not relevant for comparisons with Articles 10, 11, 12, 18, and 36 of PHIPA. In addition, Articles 38(2) and 39(1)(2) of FIPPA and Articles 10, 11, 12, 18, 32, 37, 38 and 44 of PHIPA are not related to each other (case 1).

Pair-wise comparison of Article 38(2) with Article 29 returns a case 3 (see Table E.21), while it returns a case 1 for Article 31 and a case 5 for Article 36. Pair-wise comparison of Articles 39(1),(2) with Articles 29, 31 and 36 all return a case 1.

Table E.21: Pair-Wise Comparison of Article 38(2) of FIPPA and Article 29 of PHIPA

Statement	**Statement**$_1$	**Statement**$_2$	Comparison
Section	Collection of personal information	Requirement for consent	-
Actor	A person	An HIC	A person belongs to an HIC
Modal Verb	Shall	Shall	Same
Clause	Not Collect personal information on behalf of an institution	[Not] collect, use or disclose PHI about an individual	same
Exception	The collection is expressly authorized by statute, used for the purposes [...]	May collect, use or disclose PHI	exception1 is similar to exception of PHIPA plus precondition 2
Precondition 1	-	It has the individual's consent, and the collection, use or disclosure [...] is necessary (or)	addition
Precondition 2	Statement d	The collection, use or disclosure is [...] permitted	-
XRef	Despite PHIPA	-	

Pair-wise comparison of Article 41(1d) and Article 29 is shown in Table E.22. The result illustrates case 5, which is the same result obtained when comparing it to Article 31.

Table E.22: Pair-Wise Comparison of Article 41(1d) of FIPPA and Article 29 of PHIPA

Statement	**Statement**$_1$	**Statement**$_2$	Comparison
Section	Use of personal information	Requirement for consent	-
Actor	An institution	An HIC	
Modal Verb	Shall	Shall	
Clause	Not use Personal information [...]	[Not] collect, use or disclose PHI about an individual	
Exception	May Use	May collect, use or disclose PHI	
Precondition 1	-	It has the individual's consent, and the collection, use or disclosure [...] is necessary (or)	
Precondition 2	Statement d	The collection, use or disclosure is [...] permitted	
XRef	Despite PHIPA	-	

Pair-wise comparisons of Articles 41 and 42 with Articles 38 and 44 of PHIPA result in case 1. Pair-wise analysis of Article 41 with Articles 32 and 37 lead to case 5. Finally, the comparison of Article 42 with Article 32 is a case 3, whereas with Articles 29, 31 and 37 the result is case 1.

E.7 Pair-Wise Comparison of PHIPA with HCCA

In this section, we compare Articles 10 (Information practices), 11 (Accuracy), 12 (Security), 18 (Elements of consent), 29 (Requirement for consent), 31 (Use and disclosure of personal health information), 32 (Disclosure for fundraising), parts of 36 (Indirect collection) (statements 1a-d), parts of 37 (Permitted Use) (statements 1a,1d, 1i and 3), 38 (Disclosures related to providing health care) (statements 1a and 2), and parts of 44 (Disclosure for research)(statements 1-6) of PHIPA with Articles 10(1) (Consent to Treatment) and 11 (1)(4) (Elements of consent) of HCCA.

In the first pass, based on the step for finding the matching sections of the two regulations, we identify that Articles 10 and 11 do not have anything in common with Articles 10, 11, 12, 29, 31, 32, 36, 37, 38 and 44. For the remaining pairs, comparisons

return a case 2 between Article 11(1)(4) and Article 18, and a case 1 between Article 10(1) and Article 18.

Bibliography

[1] Allen, L. E. Symbolic logic: A razor-edged tool for drafting and interpreting legal documents. *The Yale Law Journal 66* (195), 833–879.

[2] Amyot, D., Ghanavati, S., Horkoff, J., Mussbacher, G., Peyton, L., and Yu, E. S. K. Evaluating goal models within the goal-oriented requirement language. *Int. J. Intell. Syst. 25* (August 2010), 841–877.

[3] Amyot, D., Horkoff, J., Gross, D., and Mussbacher, G. A lightweight GRL profile for i* modeling. In *Proceedings of the ER 2009 Workshops (CoMoL, ETheCoM, FP-UML, MOST-ONISW, QoIS, RIGiM, SeCoGIS) on Advances in Conceptual Modeling - Challenging Perspectives* (Berlin, Heidelberg, 2009), ER '09, Springer-Verlag, pp. 254–264.

[4] Amyot, D., and Mussbacher, G. User Requirements Notation: The first ten years, the next ten years (invited paper). *Journal of Software (JSW) 6*, 5 (2011), 747–768.

[5] Antoniou, G., Billington, D., and Maher, M. J. On the analysis of regulations using defeasible rules. In *Proceedings of the Thirty-second Annual Hawaii International Conference on System Sciences, Volume 6* (Washington, DC, USA, 1999), IEEE Computer Society, pp. 6033–.

[6] Ballant, D., Belpaire, C., Darimont, R., Delor, E., Genard, D., Nève, C., Roussel, J.-L., and Vanbrabant, A. Requirements engineering with

GRAIL/KAOS: From goal analysis to automatically derived requirements documents. In *11th IEEE International Requirements Engineering Conference (RE'03)* (USA, 2003).

[7] Barbuceanu, M. A negotiation shell. In *Agents* (1999), pp. 348–349.

[8] Barth, A., Datta, A., Mitchell, J. C., and Nissenbaum, H. Privacy and contextual integrity: Framework and applications. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (Washington, DC, USA, 2006), IEEE Computer Society, pp. 184–198.

[9] Boella, G., and van der Torre, L. Permissions and obligations in hierarchical normative systems. In *Proceedings of the 9th international conference on Artificial intelligence and law* (New York, NY, USA, 2003), ICAIL '03, ACM, pp. 109–118.

[10] Breaux, T., Antón, A., Boucher, K., and Dorfman, M. Legal requirements, compliance and practice: An industry case study in accessibility. In *International Requirements Engineering, 2008. RE '08. 16th IEEE* (sept. 2008), pp. 43 –52.

[11] Breaux, T. D., and Antón, A. I. Analyzing goal semantics for rights, permissions, and obligations. In *RE* (2005), IEEE Computer Society, pp. 177–188.

[12] Breaux, T. D., and Antón, A. I. An algorithm to generate compliance monitors from regulations. Tech. Rep. TR-2006-9, NC State Computer Science, March 2006.

[13] Breaux, T. D., Antón, A. I., and Spafford, E. A distributed requirements management framework for legal compliance and accountability. *Journal of Computers and Security 28* (2009), 8–17.

[14] Breaux, T. D., Vail, M. W., and Antón, A. I. Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In

14th IEEE Int. Conf. on Requirements Engineering (RE'06) (USA, 2006), pp. 46–55.

[15] Cai, Z., and Yu, E. S. K. Addressing performance requirements using a goal and scenario-oriented approach. In *Advanced Information Systems Engineering*, A. Pidduck, M. Ozsu, J. Mylopoulos, and C. Woo, Eds., vol. 2348 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2006, pp. 706–710.

[16] Chung, L., Nixon, B. A., Yu, E. S. K., and Mylopoulos, J. *Non-Functional Requirements in Software Engineering*, vol. 5 of *International Series in Software Engineering*. Springer, 1999.

[17] Cleven, A., and Winter, R. Regulatory compliance in information systems research - literature analysis and research agenda. In *Enterprise, Business-Process and Information Systems Modeling*, vol. 29 of *LNBIP*. Springer, 2009, pp. 174–186.

[18] CSA. Canadian Standards Association Model Code for the Protection of Personal Information. `http://www.csa.ca/cm/ca/en/privacy-code`, 2011. [Online; accessed November 2012].

[19] Darimont, R., Delor, E., Massonet, P., and van Lamsweerde, A. GRAIL/KAOS: an environment for goal-driven requirements engineering. In *Proceedings of the 19th international conference on Software engineering* (New York, NY, USA, 1997), ICSE '97, ACM, pp. 612–613.

[20] Department of Justice. Privacy act (r.s.c., 1985, c. p-21). `http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html`, 1985. [Online; accessed November 2012].

[21] Easterbrook, S., and Nuseibeh, B. Managing inconsistencies in an evolving specification. In *Requirements Engineering, 1995., Proceedings of the Second IEEE International Symposium on* (mar 1995), pp. 48 – 55.

[22] Finkelstein, A., Gabbay, D., Hunter, A., Kramer, J., and Nuseibeh, B. Inconsistency handling in multiperspective specifications. *Software Engineering, IEEE Transactions on 20*, 8 (aug 1994), 569 –578.

[23] Ghanavati, S. A compliance framework for business processes based on URN. M.Sc. thesis, School of Information Technology and Engineering, University of Ottawa, Canada, 2007.

[24] Ghanavati, S., Amyot, D., and Peyton, L. A requirements management framework for privacy compliance. In *Proc. of the 10th Workshop on Requirements Engineering (WER'07)* (Canada, 2007), pp. 149–159.

[25] Ghanavati, S., Amyot, D., and Peyton, L. Towards a framework for tracking legal compliance in healthcare. In *19th Int. Conf. on Advanced Information Systems Engineering (CAiSE'07)*, vol. 4495 of *LNBIP*. Springer, Norway, 2007, pp. 218–232.

[26] Ghanavati, S., Amyot, D., and Peyton, L. Compliance analysis based on a goal-oriented requirement language evaluation methodology. In *17th Int. Conf. on Requirements Engineering (RE'09)* (USA, 2009), pp. 133–142.

[27] Ghanavati, S., Amyot, D., and Peyton, L. A systematic review of goal-oriented requirements management frameworks for business process compliance. In *Requirements Engineering and Law (RELAW), 2011 Fourth International Workshop on* (2011), pp. 25–34.

[28] Ghanavati, S., Amyot, D., Siena, A., Susi, A., and Perini, A. Towards a framework for business process compliance. In *14th IEEE International Workshop on Enterprise Distributed Object Computing Conference Workshops (EDOCW'10)* (Brazil, 2010), pp. 330–334.

[29] Ghanavati, S., Siena, A., Amyot, D., Susi, A., and Perini, A. Making business processes law-compliant. In *1st Workshop on Law Compliancy Issues in Organisational Systems and Strategies (iComply'10)* (Italy, 2010), pp. 1–5.

[30] Giorgini, P., Massacci, F., Mylopoulos, J., and Zannone, N. Modeling security requirements through ownership, permission and delegation. In *Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on* (2005), pp. 167–176.

[31] Giorgini, P., Mylopoulos, J., and Sebastiani, R. Goal-oriented requirements analysis and reasoning in the Tropos methodology. *Eng. Appl. Artif. Intell. 18* (March 2005), 159–171.

[32] Goedertier, S., and Vanthienen, J. Designing compliant business processes with obligations and permissions. In *Business Process Management Workshops*, vol. 4103 of *Lecture Notes in Computer Science*. 2006, pp. 5–14.

[33] Gordon, D., and Breaux, T. Comparing requirements from multiple jurisdictions. In *Requirements Engineering and Law (RELAW), 2011 Fourth International Workshop on* (aug. 2011), pp. 43 –49.

[34] Gordon, D., and Breaux, T. Reconciling multi-jurisdictional legal requirements: A case study in requirements water marking. In *Requirements Engineering Conference (RE), 2012 20th IEEE International* (sept. 2012), pp. 91 –100.

[35] Gordon, D. G., and Breaux, T. D. Managing multi-jurisdictional requirements in the cloud: towards a computational legal landscape. In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop* (New York, NY, USA, 2011), CCSW '11, ACM, pp. 83–94.

[36] Governatori, G., Rotolo, A., and Sartor, G. Temporalised normative positions in defeasible logic. In *Proceedings of the 10th international conference*

on Artificial intelligence and law (New York, NY, USA, 2005), ICAIL '05, ACM, pp. 25–34.

[37] Government of Canada. Personal Information Protection and Electronic Documents Act (PIPEDA). `http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html`, 2011. [Online; accessed November 2012].

[38] Government of Ontario. Health Care Consent Act (HCCA), 1996. `http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_96h02_e.htm`, 1996. [Online; accessed January 2013].

[39] Government of Ontario. Quality of Care Information Protection Act (QoCIPA), 2004. `http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04q03_e.htm`, 2004. [Online; accessed January 2013].

[40] Government of Ontario. Personal Health Information Protection Act (PHIPA), 2004. `http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm#BK39`, 2011. [Online; accessed November 2012].

[41] Grau, G., Horkoff, J., and Schmitz, D. Available *i** tools. `http://istar.rwth-aachen.de/tiki-index.php?page=i%2A+Tools`, 2011. [Online; accessed 2-May-2011].

[42] Halas, H., Porekar, J., Klobučar, T., and Blazič, A. J. Organizational aspect of trusted legally valid long-term electronic archive solution. *WSEAS Trans. Info. Sci. and App. 5* (2008), 939–948.

[43] Hamou-Lhadj, A., and Hamou-Lhadj, A. Towards a compliance support framework for global software companies. In *Proc. of the 11th IASTED Int. Conf. on Software Engineering and Applications* (USA, 2007), pp. 31–36.

[44] Hassan, W., and Logrippo, L. Requirements and compliance in legal systems: a logic approach. In *1st Int. Workshop on Requirements Engineering and Law (RELAW'08)* (Spain, 2008), pp. 40–44.

[45] Hassan, W., and Logrippo, L. Validating compliance with privacy legislation. *Journal of Information Systems Frontiers (In Press)* (2008). [Online; accessed January 2013].

[46] Hassan, W., and Logrippo, L. Governance requirements extraction model for legal compliance validation. In *2nd Int. Workshop on Requirements Engineering and Law (RELAW'09)* (USA, 2009), IEEE CS, pp. 7–12.

[47] Hevner, A. R., March, S. T., Park, J., and Ram, S. Design science in information systems research. *Management Information Systems Quarterly 28*, 1 (2004), 75–106.

[48] Horkoff, J., and Yu, E. S. K. Qualitative, interactive, backward analysis of i* models. In *iStar* (2008), J. B. de Castro, X. Franch, A. Perini, and E. S. K. Yu, Eds., vol. 322 of *CEUR Workshop Proceedings*, CEUR-WS.org, pp. 43–46.

[49] Horkoff, J., and Yu, E. S. K. Analyzing goal models: different approaches and how to choose among them. In *SAC* (2011), W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds., ACM, pp. 675–682.

[50] Horty, J. F. *Agency and Deontic Logic*. Oxford University Press, 2001.

[51] Ingolfo, S., Mylopoulos, J., Perini, A., Siena, A., and Susi, A. Nòmos: from strategic dependencies to obligations. In *iStar* (2011), pp. 72–77.

[52] Ishikawa, F., Inoue, R., and Honiden, S. Modeling, analyzing and weaving legal interpretations in goal-oriented requirements engineering. In *Proceedings of the 2009 Second International Workshop on Requirements Engineering and Law* (Washington, DC, USA, 2009), RELAW '09, IEEE Computer Society, pp. 39–44.

[53] ITU-T. Recommendation Z.151 (11/08): User Requirements Notation (URN) – Language Definition. `http://www.itu.int/rec/T-REC-Z.151/en`, 2008.

[54] Karagiannis, D. A business process-based modelling extension for regulatory compliance. In *Multikonferenz Wirtschaftsinformatik (MKWI'08)* (2008), pp. 1159–1173.

[55] Kerrigan, S., Lau, G., Zhou, L., Wiederhold, G., and Law, K. H. Information infrastructure for regulation management and compliance checking. In *In The First National Conference on Digital Government* (2001), pp. 167–170.

[56] Kharbili, M. E., and Pulvermüller, E. A semantic framework for compliance management in business process management. In *Business Process, Services Computing and Intelligent Service Management* (2009), vol. 147 of *LNI*, GI, pp. 60–80.

[57] Kharbili, M. E., Stein, S., Markovic, I., and Pulvermüller, E. Towards a framework for semantic business process compliance management. In *Proc. 1st International Workshop on Governance, Risk and Compliance - Applications in Information Systems (GRCIS'08)* (2008), vol. 339 of *CEUR-WS*, pp. 1–15.

[58] Kitchenham, B., and Charters, S. Guidelines for performing systematic literature reviews in software engineering, version 2.3. Tech. rep., Keele Univ. and Univ. of Durham, 2007.

[59] Krausova, A., Massacci, F., and Saidane, A. Legal patterns implement trust in it requirements: When legal means are the "best" implementation of it technical goals. In *2nd Int. Workshop on Requirements Engineering and Law (RELAW'09)* (USA, 2009), pp. 33–38.

[60] Lamsweerde, A. v. Goal-oriented requirements enginering: A roundtrip from research to practice. In *Proceedings of the Requirements Engineering Conference,*

12th IEEE International (Washington, DC, USA, 2004), IEEE Computer Society, pp. 4–7.

[61] Lapouchnian, A. Goal-oriented requirements engineering: An overview of the current research. Depth report, Department of Computer Science, University of Toronto, Canada, 2005.

[62] Lapouchnian, A., and Lesperance, Y. Modeling mental states in agent-oriented requirements engineering. In *Advanced Information Systems Engineering*, E. Dubois and K. Pohl, Eds., vol. 4001 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2006, pp. 480–494.

[63] Lapouchnian, A., Yu, Y., and Mylopoulos, J. Requirements-driven design and configuration management of business processes. In *Proceedings of the 5th international conference on Business process management* (Berlin, Heidelberg, 2007), BPM'07, Springer-Verlag, pp. 246–261.

[64] Lau, G. T., Law, K. H., and Wiederhold, G. Legal information retrieval and application to e-rulemaking. In *Proceedings of the 10th international conference on Artificial intelligence and law* (New York, NY, USA, 2005), ICAIL '05, ACM, pp. 146–154.

[65] Letier, E., and van Lamsweerde, A. Reasoning about partial goal satisfaction for requirements and design engineering. In *SIGSOFT FSE* (2004), R. N. Taylor and M. B. Dwyer, Eds., ACM, pp. 53–62.

[66] Liu, L., and Yu, E. S. K. From requirements to architectural design - using goals and scenarios. In *STRAW'01* (2001), pp. 1–.

[67] Logrippo, L. From e-business to e-laws and e-judgments: 4,000 years of experience. In *Proc. of the Second International Conference on Technical and Legal Aspects of the e-Society (CYBERLAWS'11)* (2011), pp. 22–28.

[68] Loniewski, G., Insfrán, E., and Abrahão, S. A systematic review of the use of requirements engineering techniques in model-driven development. In *MoDELS (2)* (2010), D. C. Petriu, N. Rouquette, and Ø. Haugen, Eds., vol. 6395 of *Lecture Notes in Computer Science*, Springer, pp. 213–227.

[69] Lu, R., Sadiq, S., and Governatori, G. Compliance aware business process design. In *Proceedings of the 2007 international conference on Business process management* (Berlin, Heidelberg, 2008), BPM'07, Springer-Verlag, pp. 120–131.

[70] Luo, H., and Amyot, D. Towards a declarative, constraint-oriented semantics with a generic evaluation algorithm for GRL. In *5th International i* Workshop* (2011), vol. 766 of *CEUR Workshop Proceedings*, pp. 26–31.

[71] Massey, A., Otto, P., Hayward, L., and Antón, A. I. Evaluating existing security and privacy requirements for legal compliance. *Special Issue on RE'09: Security Requirements Engineering, REJ 15* (2010), 119–137.

[72] Massey, A. K., Otto, P. N., and Antón, A. I. Prioritizing legal requirements. *2nd Int. Workshop on Requirements Engineering and Law (RELAW'09)* (2009), 27–32.

[73] Maxwell, J., Antón, A., and Swire, P. A legal cross-references taxonomy for identifying conflicting software requirements. In *Requirements Engineering Conference (RE), 2011 19th IEEE International* (29 2011-sept. 2 2011), pp. 197 –206.

[74] Maxwell, J. C., and Antón, A. I. Checking existing requirements for compliance with law using a production rule model. In *2nd Int. Workshop on Requirements Engineering and Law (RELAW'09)* (USA, 2009), pp. 1–6.

[75] Maxwell, J. C., and Antón, A. I. Developing production rule models to aid in acquiring requirements from legal texts. In *17th Int. Conf. on Requirements Engineering (RE'09)* (USA, 2009), pp. 101–110.

[76] Maxwell, J. C., and Antón, A. I. The production rule framework: developing a canonical set of software requirements for compliance with law. In *Proceedings of the 1st ACM International Health Informatics Symposium* (New York, NY, USA, 2010), IHI '10, ACM, pp. 629–636.

[77] Ministry of Health and Long-Term Care, Ontario. Personal Health Information Protection Act, 2004: An overview. `http://www.health.gov.on.ca/english/providers/legislation/priv_legislation/overview_leg.pdf`, 2004. [Online; accessed November 2012].

[78] Ministry of Health and Long-Term Care, Ontario. Municipal freedom of information and protection of privacy act. `http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm#BK48`, 2007. [Online; accessed November 2012].

[79] Ministry of Health and Long-Term Care, Ontario. Freedom of information and protection of privacy act. `http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm#BK63`, 2011. [Online; accessed November 2012].

[80] Mussbacher, G., and Amyot, D. Goal and scenario modeling, analysis, and transformation with jUCMNav. In *ICSE Companion* (2009), IEEE, pp. 431–432.

[81] Mylopoulos, J., Chung, L., and Yu, E. S. K. From object-oriented to goal-oriented requirements analysis. *Commun. ACM 42* (January 1999), 31–37.

[82] Oates, B. J. *Researching Information Systems and Computing*. Sage Publications Ltd., 2006.

[83] Otto, P. N., and Antón, A. I. Addressing legal requirements in requirements engineering. *15th IEEE Int. Conf. on Requirements Engineering (RE'10)* (2007), 5–14.

[84] Perry, D. E., Porter, A. A., and Votta, L. G. Empirical studies of software engineering: a roadmap. In *Proceedings of the Conference on The Future of Software Engineering* (New York, NY, USA, 2000), ICSE '00, ACM, pp. 345–355.

[85] Pourshahid, A., Amyot, D., Peyton, L., Ghanavati, S., Chen, P., Weiss, M., and Forster, A. J. Business process management with the User Requirements Notation. *Electronic Commerce Research 9* (December 2009), 269–316.

[86] Rifaut, A. Compliance management with measurement frameworks. In *Requirements Engineering and Law (RELAW), 2011 Fourth International Workshop on* (2011), IEEE CS, pp. 15 –24.

[87] Rifaut, A., and Dubois, E. Using goal-oriented requirements engineering for improving the quality of ISO/IEC 15504 based compliance assessment frameworks. In *16th Int. Conf. on Requirements Engineering (RE'08)* (Spain, 2008), pp. 33–42.

[88] Rifaut, A., and Ghanavati, S. Measurement-oriented comparison of multiple regulations with GRL. In *Requirements Engineering and Law (RELAW), 2012 Fifth International Workshop on* (2012), pp. 7–16.

[89] Robinson, W., and Fickas, S. Supporting multi-perspective requirements engineering. In *Requirements Engineering, 1994., Proceedings of the First International Conference on* (apr 1994), pp. 206 –215.

[90] Roy, J.-F. Requirement engineering with URN: Integrating goals and scenarios. M.sc. thesis, School of Information Technology and Engineering (SITE), University of Ottawa, Canada, 2007.

[91] Roy, J.-F., Kealey, J., and Amyot, D. Towards integrated tool support for the user requirements notation. In *System Analysis and Modeling: Language Profiles*, R. Gotzhein and R. Reed, Eds., vol. 4320 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2006, pp. 198–215.

[92] Saaty, T. L. Decision making with the analytic hierarchy process. *International Journal of Services Sciences 1*, 1 (2008), 83–98.

[93] Sartor, G. Fundamental legal concepts: A formal and teleological characterisation. *Artificial Intelligence and Law 14* (2006), 101–142.

[94] Schleicher, D., Anstett, T., Leymann, F., and Schumm, D. Compliant business process design using refinement layers. In *OTM Conferences (1)* (2010), R. Meersman, T. S. Dillon, and P. Herrero, Eds., vol. 6426 of *Lecture Notes in Computer Science*, Springer, pp. 114–131.

[95] Shamsaei, A. *Indicator-based Policy Compliance of Business Processes*. PhD thesis, School of Electrical Engineering and Computer Science, University of Ottawa, Canada, 2012.

[96] Shamsaei, A., Amyot, D., and Pourshahid, A. A systematic review of compliance measurement based on goals and indicators. In *Advanced Information Systems Engineering Workshops*, C. Salinesi and O. Pastor, Eds., vol. 83 of *Lecture Notes in Business Information Processing*. Springer Berlin Heidelberg, 2011, pp. 228–237.

[97] Shamsaei, A., Amyot, D., Pourshahid, A., Mussbacher, G., Tawhid, R., Yu, E., Braun, E., and Cartwright, N. An approach to specify and analyze goal model families. In *7th System Analysis and Modelling (SAM)*, vol. 7744 of *Lecture Notes in Computer Science*. Springer, 2012.

[98] Shamsaei, A., Pourshahid, A., and Amyot, D. Business process compliance tracking using key performance indicators. In *Business Process Management Workshops*, M. Muehlen and J. Su, Eds., vol. 66 of *Lecture Notes in Business Information Processing*. Springer Berlin Heidelberg, 2011, pp. 73–84.

[99] Siena, A. *Engineering Law-Compliant Requirements: The* Nòmos *Framework.* Phd thesis, Department of Information Engineering and Computer Science, University of Trento, Italy, 2010.

[100] Siena, A., Jureta, I., Ingolfo, S., Susi, A., Perini, A., and Mylopoulos, J. Capturing variability of law with nómos 2. In *Conceptual Modeling*, P. Atzeni, D. Cheung, and S. Ram, Eds., vol. 7532 of *Lecture Notes in Computer Science.* Springer Berlin Heidelberg, 2012, pp. 383–396.

[101] Siena, A., Maiden, N., Lockerbie, J., Karlsen, K., Perini, A., and Susi, A. Exploring the effectiveness of normative i* modelling: Results from a case study on food chain traceability. In *Proceedings of the 20th international conference on Advanced Information Systems Engineering* (Berlin, Heidelberg, 2008), CAiSE '08, Springer-Verlag, pp. 182–196.

[102] Siena, A., Mylopoulos, J., Perini, A., and Susi, A. From laws to requirements. In *1st Int. Workshop on Requirements Engineering and Law (RELAW'08)* (Spain, 2008), pp. 6–10.

[103] Siena, A., Mylopoulos, J., Perini, A., and Susi, A. Designing law-compliant software requirements. *Conceptual Modeling-ER 2009* (2009), 472–486.

[104] Siena, A., Perini, A., Susi, A., and Mylopoulos, J. A Meta-Model for Modelling Law-Compliant Requirements. In *2nd Int. Workshop on Requirements Engineering and Law (RELAW'09)* (USA, 2009), pp. 45–51.

[105] Siena, A., Perini, A., Susi, A., and Mylopoulos, J. Towards a framework for law-compliant software requirements. In *31st Int. Conf. on Software Engineering (ICSE'09),* (2009), IEEE, pp. 251–254.

[106] U.S. Government. Health Insurance Portability and Accountability Act (HIPAA). `http://www.hhs.gov/ocr/privacy/`, 1996. [Online; accessed November 2012].

[107] van Lamsweerde, A., Darimont, R., and Letier, E. Managing conflicts in goal-driven requirements engineering. *Software Engineering, IEEE Transactions on 24*, 11 (nov 1998), 908 –926.

[108] Weiss, M., and Amyot, D. Business model design and evolution, 2005.

[109] Weiss, M., and Amyot, D. Design and evolution of e-business models. In *Proceedings of the Seventh IEEE International Conference on E-Commerce Technology* (Washington, DC, USA, 2005), IEEE Computer Society, pp. 462–466.

[110] Weiss, M., and Amyot, D. Designing and evolving business models with URN. In *Proc. of Montreal Conference on eTechnologies (MCETECH05)* (2005), pp. 149–162.

[111] Wenar, L. Rights. `http://plato.stanford.edu/entries/rights/`, 2004. [Online; accessed 15-July-2011].

[112] Wikipedia. Data protection directive. `http://en.wikipedia.org/wiki/Data_Protection_Directive`, 2011. [Online; accessed November 2012].

[113] Young, J., and Antón, A. I. Identifying commitment-based software requirements to thwart unfair and deceptive practices. In *2nd Int. Workshop on Requirements Engineering and Law (RELAW'09)* (2009), pp. 19–20.

[114] Young, J., and Antón, A. I. A method for identifying software requirements based on policy commitments. In *18th Int. Conf. on Requirements Engineering (RE'10)* (2010), pp. 47–56.

[115] Yu, E. S. K. Towards modeling and reasoning support for early-phase requirements engineering. In *Proceedings of the 3rd IEEE International Symposium on Requirements Engineering* (Washington, DC, USA, 1997), RE '97, IEEE Computer Society, pp. 226–235.

[116] Yu, E. S. K. Why agent-oriented requirements engineering. In *REFSQ'97 - Requirements Engineering: Foundation of Software Quality* (1997), Presses Universitaires de Namur.

[117] Yu, E. S. K. Agent orientation as a modelling paradigm. *Wirtschaftsinformatik 43*, 3 (April 2001), 123–132.