A Legal Perspective on Business: Modeling the Impact of Law

Sepideh Ghanavati [1], Alberto Siena [2], Anna Perini [2], Daniel Amyot [1], Liam Peyton [1],
and Angelo Susi [2]

[1] SITE, University of Ottawa, Canada
{sghanava, damyot, lpeyton}@site.uottawa.ca
[2] University of Trento, Italy
{siena, perini, susi}@itc.it

Abstract. Modern goal-oriented requirements engineering frameworks use modeling as a means of better understanding a domain, leading to an overall improvement in the quality of the requirements. Regulations and laws impose additional context and constraints on software goals and can limit the satisfaction of stakeholder needs. Organizations and software developers need modeling tools that can properly address the potential deep impact legal issues can have on the effectiveness of business strategies. In this paper, we perform a preliminary study into the development of a modeling framework able to support the analysis of legal prescriptions alongside business strategies. We demonstrate, via an example drawn from a case study of the Health Insurance Portability and Accountability Act (HIPAA), how models of this law can be built with the GRL modeling language and how they can be evaluated as part of the business goal models.

Keywords: Business Modeling, Goal-oriented Requirement Language, HIPAA, Law Modeling

1 Introduction

In the development of modern information systems, understanding and analyzing the purpose of a software system before defining its desired functionality is becoming more and more important [6]. The early requirements analysis phase [9] is the part of the software development process in which it is possible to effectively understand the justification and need for a new system with respect to the organizational setting in which it will operate. In this phase, the needs of the stakeholders are taken into consideration. The business strategies define possibly the most important needs of an organization, and are likely the driving force behind the development initiative [15]. In this context, the goal-oriented techniques proposed in the last decade [14][10] try to answer software *why* questions in addition to the standard *what* and *how* as they relate to system functionality. Answers to *why* questions will ultimately link software requirements to stakeholder needs, preferences and objectives.

Goal analysis techniques [3] are useful in order to understand the structure and the correlations between goals, their decomposition into more fine-grained sub-goals, and their relationship with operational plans. Moreover, reasoning techniques applied to goal models [5] can be very useful in verifying model properties and have shown to be useful for analysts in conflict resolution processes that weigh the different aspects of a strategy [15] and work to improve the decisions made about the models.

Although these techniques are very helpful when reasoning about models with a single goal, they are inadequate in the support of strategic decisions of a real multi-goal organization. This is mainly due to the fact that they are typically built from the perspective of the system stakeholders and do not consider other dimensions like the impact of laws on the organizational strategy. For example, ignoring legal prescriptions may lead to a set of requirements that is fully aligned to stakeholders needs, but that is in violation of the law. Such a situation will eventually result in the need for later correction of the requirements and increased costs.

In recent years, there have been some attempts to apply goal modeling techniques to the setting of legal documents. However, there are still no complete guidelines for how this can be performed. Furthermore, no analysis has ever been done in order to measure the precision and completeness of any such model.

In this paper, we analyze the capabilities and limitations of the Goal-oriented Requirements Language (GRL) [13] for legal documents. In addition, we discuss the impact of these models on an organization in terms of the possible decisions an organization can make to satisfy the law and still accomplish their business objectives.

The paper is structured as follows: Section 2 discusses work related to legal goal modeling and its impact on business processes. Section 3 details the steps that need to be taken to model legal documents whereas Section 4 illustrates these steps and analyzes the pros and cons of different goal models with the help of a case study affected by the Health Insurance Portability and Accountability Acts (HIPAA). Finally, in Section 5, we analyze the impact of a legal model on an organizational goal model and in Section 6 we present our conclusions.

2 Related Work

In recent years, research has been undertaken to investigate the role of laws in software requirements engineering processes. Antón and Breaux, in [1], developed a systematic process for extracting rights and obligations (including auxiliary concepts such as actors and constraints) from legal texts thereby generating a formal model of law. This work provides an important example of the scale and complexity involved when dealing with the vagueness of legal sources.

In terms of organized legal concepts, we have the LRI-Core [2]. This describes a layered legal ontology, built from a foundational ontology that is instantiated as a domain ontology. LRI-Core is based on the idea that the law is driven by common world concepts and words, and as such the ontology defines concepts such as agent, action and organization together with legal concepts.

The need for legal modeling is also implicitly contained in other works that strive to perform requirements modeling. Darimont and Lemoine use KAOS to model objectives extracted from regulatory texts [4]. Such approaches are based on the similarities between regulations and requirements. Other similar approaches come in the form of the techniques adopted in [7], where a goal model is used to model the goals and activities prescribed by laws. Ghanavati et al. in [7] built their work on the intuition that there is a need to use the same modeling notation for both the regulations and the organizational processes. As such, traceability links have been established between the law and the business processes, thus enabling the management of their evolution. The special consideration needed to handle evolving requirements and laws are described in [8].

Other frameworks include the Normative *i** framework [16] and Secure Tropos [11]. The Normative *i** framework allows for modeling laws inside an intentional framework and produces effective additions to the requirements system. Secure Tropos constitutes a security-enhanced version of the Tropos methodology and introduces the concepts of service ownership and delegation. In order to ensure access control, strategic dependencies are refined with the conditions of permission and commitment.

With respect to these approaches, this paper studies the modeling of law and its limitations, as well as the impact that laws have on business strategies, and attempts to do so in a quantitative manner.

3 Legal Modeling

Generally speaking, laws deal with prescribing how the world *should* be and as such relate to their deontics. Moreover, laws are very complex artifacts and are hard to capture because they are expressed in natural language and are intentionally vague in order to support as of yet unseen circumstances. There are also the implications of case law which constitute instances of applied law and serve to refine written laws and dictate how they should be interpreted. Requirements modeling languages and processes are not intended to capture this level of complexity. Currently there is no precise approach in dealing with this problem from the literature.

The modeling of legal concepts has gained the attention of some researchers. In [7] the authors suggest to model legal concepts with Goal-oriented Requirements Language (GRL), which is part of the User Requirements Notation (URN). However, they ignore the possibility of using Use Case Maps (UCM), another complementary notation of URN for modeling laws and regulations since they believe that usually legal documents do dictate business processes. URN is a new ITU-T recommendation used to help capture, model, and analyze user requirements in the early stages of design. GRL is a goal modeling notation based on *i** and the Non-Functional Requirements (NFR) framework. It includes intentional elements (i.e. *goals*, *softgoals*, *tasks* and *resources*) as well as different links which connect these elements to each other. These links represent different types of relationships such as contribution, correlation, decomposition and dependency. UCM focuses mainly on the functional 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.

The benefit of using a common goal-oriented language such as GRL is that the *desired* behavior of actors (the object of legal prescriptions) can be modeled using the same language as the actual behavior. It is helpful that GRL is graphical so that it can be easily analyzed and discussed.

In fact, legal documents address the concepts of *actors*, *rights*, *obligations* and *constraints* [1]. According to Breaux et al., rights are claims that are assigned to the right bearer whereas obligations are the responsibilities applied to the obligated party and that he must fulfill in order to comply with the regulation. When an actor has a right, he has the (legal) capability to use the right to accomplish his goals. Conversely, when an actor is charged with an obligation he has the (legal) responsibility to perform the corresponding prescribed actions. It follows that the holders of rights and obligations are complementary because in order for an actor to apply a right, another actor has to perform an activity. Finally, constraints can articulate both rights and obligations which can be represented as precondition activities, exceptions or dependent obligations and rights. Therefore, a legal prescription can be described as an obligation or right statement with the provision of optional constraints.

This definition of rule statements can help us model them with GRL. Obligations, as mentioned above, are activities which must be performed by an actor in order to satisfy the goals that are described as rights attributed to another actor. In this case, there are some goals to be achieved, some tasks required to satisfy them and some actors bound to the related tasks. If the statement only contains simple rights and obligations, we can model its different parts with GRL intentional elements (softgoals, goals, tasks) and actors. If the statement contains any constraints, the constraint itself needs to be analyzed separately. Precondition activities can be modeled as tasks in GRL and linked to the related goals or tasks via contribution links of type *make, help, some positive, unknown, some negative, hurt,* or *break*.

If a constraint contains exceptional situations or actors (which usually represent nested "if" conditions), it cannot be shown with GRL, since they usually have a procedural nature while GRL is only able to depict static representations of goal models. To model these exceptions, we can use UCM instead since this notation is able to model business processes. The benefit of using UCM over other business processing modeling notations is that it has the ability to link its elements to GRL elements. In other words, tasks and actors in GRL can be linked to responsibilities and components in UCM maps.

4 HIPAA Case Study

4.1 Model of the Law

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in the USA in 1996 [12]. HIPAA includes two titles. Title 1 protects health insurance coverage for workers and Title 2 enforces the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers. In addition, Title 2 addresses the privacy and security of health data. As an example to illustrate our work, we will consider Article

§164.314 of HIPAA. This article describes “Organizational Requirements” and the contract between the covered entity and the business associate.

Article §164.314. a(1) I prescribes that “*A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.*”.

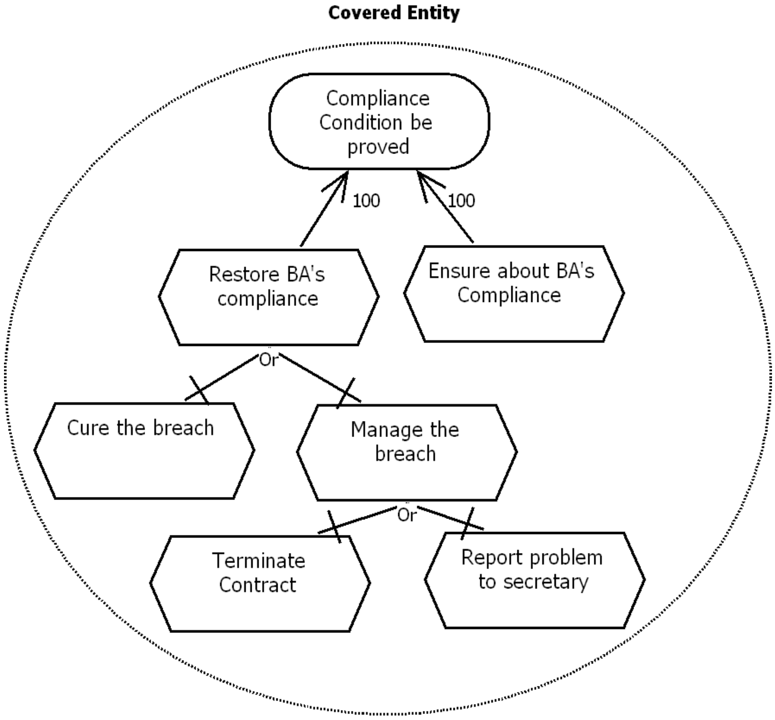
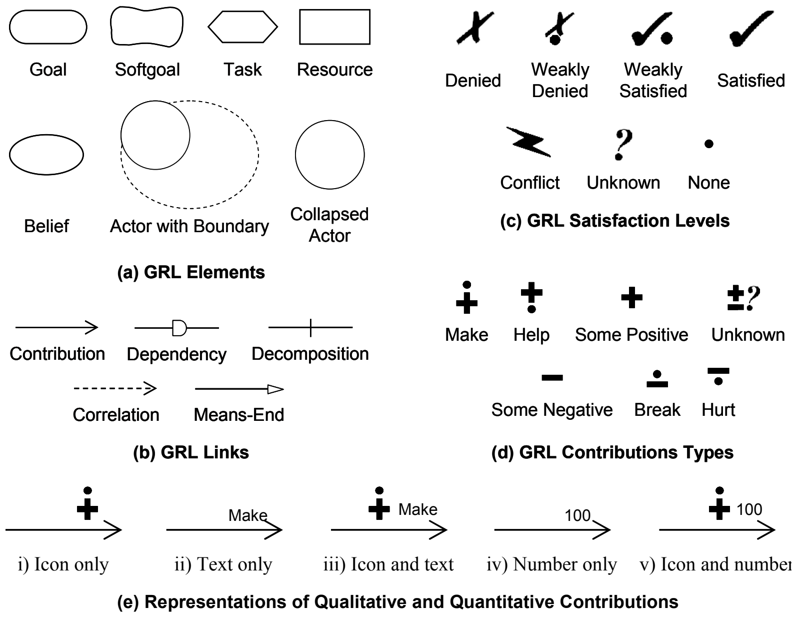


Fig. 1. GRL actor model (CE) of the Article §164.314

The main objective of this part of the article is that the covered entity complies with the standard. It introduces some key examples of the concepts we will use. The paragraph references the two role-playing actors involved, namely the Covered Entity (CE) and the Business Associate (BA). It defines the statement, “knew of a pattern of an activity and/or practice an activity which leads to material breach or violation” as a precondition for “not being in compliance.” This precondition can be modeled as a task which contributes negatively to the main objective. In other words, the BA is compliant with the standard if “the CE does not recognize any pattern of non-compliance.” Another constraint defined in the article is that “if the CE took reasonable steps to cure the breach or end the violation, the BA’s compliance will be restored." Therefore the task Cure the Breach or End the Violation will help to restore compliance. However, if it is not possible to cure the breach, the CE has to either Terminate the Contract or Report Problem to Secretary (another condition/constraint). These two tasks also contribute positively to the Restore the Breach activity. Since these two tasks are part of one condition (i.e. *if such steps were unsuccessful*), we put them as sub-tasks of the main task Manage the Breach. This portion of the article can be modeled in GRL. Figure 1 shows an excerpt of the GRL model for Article §164.314.

As mentioned above, GRL intentional elements are *softgoals*, *goals*, *tasks* and *resources*. A softgoal shown as cloud is a kind of goal that can never be concretely achieved. This type of goal represents a high-level goal of the system. In Article §164.314 we have not identified any softgoals. Goals represent the conditions which must be achieved with certainty. Here, the goal of the system is Compliance Condition be Proved. Both softgoals and goals are decomposed until they are operationalized into tasks. Tasks represent the operational solutions to the system and are shown as hexagons. Tasks are usually decomposed with AND/OR links into several sub-intentional elements. Tasks are easily identified as hexagons. For example in Figure 1, Restore BA's Compliance is a task which has been decomposed by an OR link into two other tasks Cure the Breach and Manage the Breach. Figure 2 shows a brief summary of the GRL notation elements.



(a) GRL Elements

(b) GRL Links

(c) GRL Satisfaction Levels

(d) GRL Contributions Types

(e) Representations of Qualitative and Quantitative Contributions

Fig. 2. GRL notation summary

Contribution links can also have different levels of effect on the softgoals or goals connected to them. Links of type *make*, *help*, and *some*+ indicate positive relationships that are sufficient, insufficient and unknown respectively. Those links that are labeled as *break*, *hurt* and *some*– are used for negative contributions that are respectively sufficient, insufficient and unknown. In Figure 1, both tasks Restore the Breach and Ensure about BA's Compliance have *make* contributions to the goal Compliance Condition be Proved.

The GRL model we built here has some assumptions as well as some limitations. As mentioned above, there are some tasks and activities in the GRL model such as Restore the Breach which are not explicit in the text. However, since the GRL model aims to lessen the complexity of the text, it is necessary to include some intentional elements which are only implied by the text. In addition, there are some situations in the legal text which imposes sequence and priorities for activities. For example in Article §164.314, it is written that *"if such steps were unsuccessful (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary"*. Although, these alternatives are illustrated in the GRL model, their sequence and priorities are not. In this case, we use UCM because this notation is able to model scenarios and business processes. Figure 3 illustrates a UCM which serves to model the *"if conditions"* in the legal document.

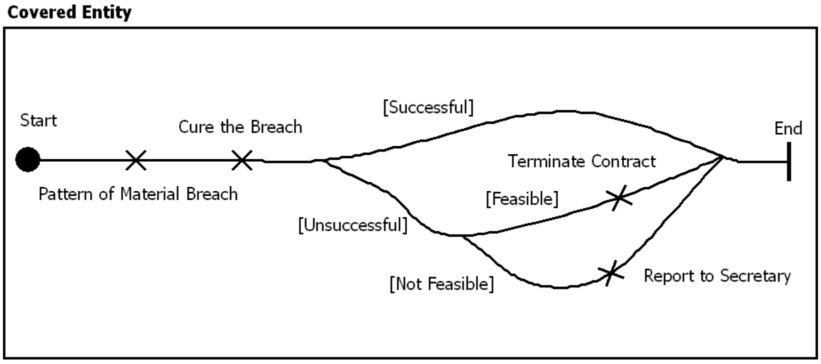


Fig. 3. UCM model of the Article §164.314

Figure 3 includes only one Use Case Map with one component called Covered Entity. This component has a link to the actor CE. There is a path from Start to End with two OR-forks to show the different possibilities. Responsibilities such as Cure the Breach that are mapped to tasks are shown by an 'X'. Conditions, such as [successful] are shown as bracketed strings.

This UCM shows in case of a breach the Covered Entity has to Cure the Breach and if this activity is not successful and if terminating the contract is feasible, the Covered Entity will Terminate the Contract, otherwise he will Report to the Secretary. By linking the related parts of this UCM map to the above GRL model, we can represent the ordering of the tasks which is critical in any analysis where dependencies exist.

4.2 GRL Model of Law: Pros and Cons

GRL is a conceptual modeling tool that allows goal-based models to be built from legal prescriptions and serves to lessen the complexity of the representation of the law. To achieve this result, we exploit the fact that legal documents contain goals that are mandatory for the addressed subjects to achieve, and activities that are the legal means for achieving these goals. As a result, we can express in GRL both the goals of the organization and the goals of the law. In addition, since GRL is tied to UCM which is used for business process modeling, the goal model of the law can impose some new requirements on the business process of the organization. However, not everything in the law can be modeled by GRL only. For example, priorities between two options cannot be shown in GRL. In this case, UCM is added to the model to show the process and priorities.

5 Impact Analysis

5.1 Model of the Organization

Ghanavati et al. in [7] mention that in order to have good traceability and be able to manage organizational compliance with law, it is beneficial to build a corporate goal model using the same notation as the model of law. As a result, the organizational model is also built with GRL. In this section, we aim to analyze how the legal goal model impacts the satisfaction of the organization's main objective. Legal prescriptions can impact the same goal differently given two scenario alternatives. In order to analyze the relative degree of impact, we can use GRL evaluation strategies. These have the capability to analyze goals quantitatively, qualitatively or as a mixture of both approaches.

The quantitative evaluation algorithm uses quantitative contributions, quantitative degrees of goal satisfaction and quantitative importance values for actors, all in the range of -100 to +100. An evaluation algorithm then propagates the effect of each into a single numerical result also in the same range of -100 and +100. The qualitative evaluation algorithm uses qualitative contribution values (i.e. *make*, *some positive, help, none, hurt, some negative, break*), qualitative degrees of satisfaction (i.e. *denied, weakly denied, weakly satisfied, satisfied, conflict, unknown, none*) and qualitative importance values (i.e. *high, medium, low, none*). Finally, the mixed evaluation algorithm includes both quantitative and qualitative values at the same time. All of these algorithms follow a bottom-up approach. In this example, drawn from our HIPAA case study, we use the quantitative evaluation strategy.

Since the legal document we are using in our case study is HIPAA, the organization that it affects is a healthcare organization. In our example, we analyze the task of disclosing Protected Health Information (PHI) to different users in different scenarios and its impact on achieving the main goal of the hospital which is to Improve the Quality of Healthcare. In our case, the hospital aims to Disclose the PHI to Researchers or Disclose the PHI to the Healthcare Assistants. Information is disclosed to the researcher in order to help him satisfy his objective which is to Do Research. Figure 4 shows an excerpt of the associated GRL goal model.

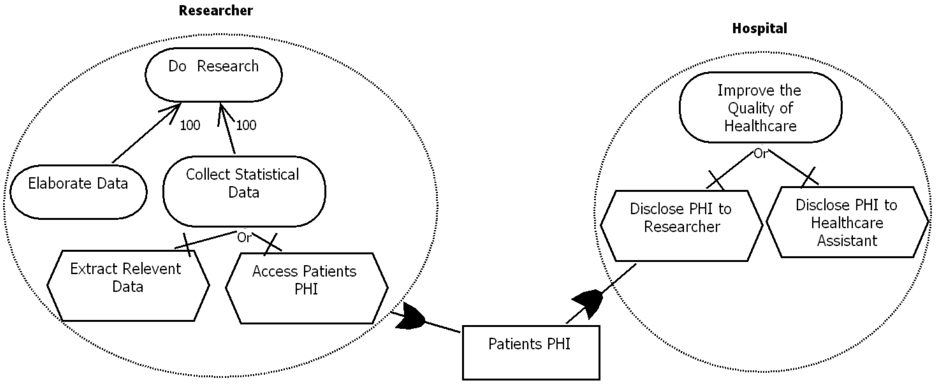


Fig. 4. Organization GRL Model

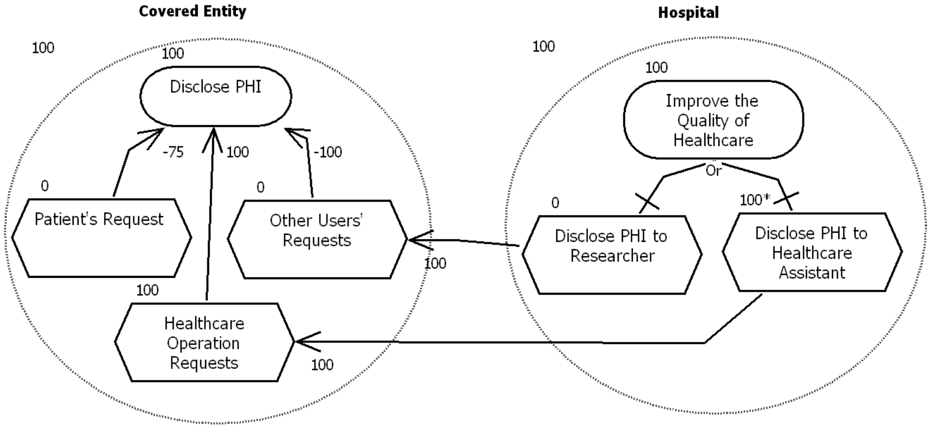
5.2 The Organization model against the Law model: a business analysis

As an example of how to analyze how the GRL model of the law affects the objectives of researchers and healthcare assistants, we define two basic scenarios. We selected these two scenarios to illustrate how modeling of law by GRL can help the organization to analyze the satisfaction of their goals. These scenarios are based on Article §164.506 which states that, *except with respect to uses or disclosures that require an authorization under §164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.* Article §164.508 specifies the exception that Article §164.506 applies, *except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section.*

Figure 5 illustrates the first scenario where a healthcare assistant wants access to PHI. In this Figure, the task Disclose PHI to Healthcare Assistant gets the value of 100. By selecting this task, the goal of the hospital, which is Improve the Quality of Healthcare, is satisfied (value of 100). According to the Article §164.506, the Covered Entity can give the permission to disclose PHI for healthcare operations, Healthcare Operation Request, which is selected with a value of 100. Therefore, Disclosing PHI to Healthcare Assistant can satisfy the main objectives of both hospital (i.e. Improve the Quality of Healthcare) and the covered entity (i.e. Disclose PHI).

In the second scenario, the Researcher wants to get access to PHI. Therefore, the task Disclose PHI to Researcher is selected and the goal Improve the Quality of Healthcare is satisfied (both shown with the value of 100). According to Article §164.508, without the authorization the researcher cannot get access to PHI.

Therefore, if the covered entity discloses data to researcher (i.e. the task Other Users' Request is satisfied), the objectives of the researcher and the hospital are satisfied but the hospital will be in breach of the law. Figure 6 illustrates this situation. The goal Disclose PHI is *denied* (unsatisfied) as it has a satisfaction level of -100. In order to comply with HIPAA, the hospital should prohibit disclosure of PHI to the researcher. However, this situation results in an unsatisfied goal of researcher and the hospital.



Covered Entity
Hospital
100
100
Disclose PHI
-75
100
-100
0
Patient's Request
0
Other Users' Requests
100
100
Healthcare Operation Requests
100
100
100
Improve the Quality of Healthcare
Or
0
100*
Disclose PHI to Researcher
Disclose PHI to Healthcare Assistant

Fig. 5. Disclosing PHI to Healthcare Assistant

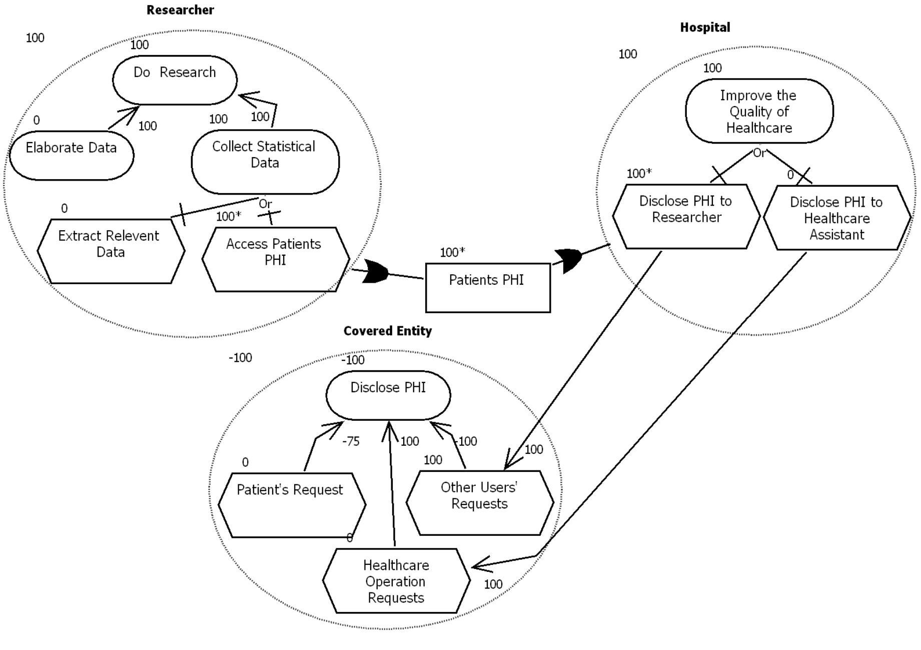


Fig. 6. Disclosing PHI to the Researcher

This impact analysis illustrates how a goal model of the law can help organizations make decisions, perform trade-off analysis, and better understand how they can achieve their internal goals and still comply with the law under which they must operate.

6 Conclusions

In this paper we have shown how the goals of an organization are affected by the law using different scenarios drawn from a case study of HIPAA. These scenarios highlighted how a modeling approach, like the one proposed here, can help formalize an organization's approach to dealing with conflicting objectives that may involve potential violations of legal responsibility. To deal with these conflicting objectives, we discussed the need for a formal goal model of the law and the necessary steps in order to create it. Such a modeling is possible if one leverages the combined capabilities of GRL and UCM, the two complementary modeling notations of URN.

In the literature, it was stated that it was not necessary to use UCM or any business process modeling languages when creating models of the law. However, with the help of a simple example, we illustrated that there exist some situations such as with conditional statements which introduce the need for options and precedence. We can model these situations as a process using the UCM notation and create links between this view and GRL's. In future, we need to provide a more comprehensive case study to explore this idea and demonstrate the necessity of UCM. It is important to note that the UCM model of law does not need to cover all aspects of the law. We only turn to the capabilities of the UCM modeling language when some procedural implication is involved.

Modeling laws manually requires a much effort in indentifying legal element, their relationships and their interpretation in a goal model. In the future, it will become important to explore and support the automatic extraction of goal models, even if only partial, from legal documents.

Acknowledgments

This work was supported by a Collaborative Health Research Project grant from CIHR and NSERC (Canada) on *Performance Management at the Point of Care: Secure Data Delivery to Drive Clinical Decision Making Processes for Hospital Quality Control*.

References

1. Breaux, T., D., Vail, M., V., and Antón, A., I.: Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations, 14th IEEE RE Conference, USA. IEEE CS, 49-58 (2006)
2. Breuker, J., Valente, A., and Winkels, R.: Legal ontologies in knowledge engineering and information management. Artificial Intelligence and Law, 12(4):241–277 (2004)

3. Dardenne, A., van Lamsweerde, A., and Fickas, S.: Goal-directed requirements acquisition. Science of Computer Programming, 20(1-2):3–50 (1993)
4. Darimont, R., Lemoine, M.: Goal-oriented analysis of regulations. In REMO 2V06: Int. Workshop on Regulations Modelling and their Verification & Validation, June, Luxemburg (2006)
5. Delor, E., Darimont, R., and Rifaut, A.: Software quality starts with the modelling of goal-oriented requirements. In 16th International Conference Software & Systems Engineering and their Applications. Paris, France, December (2003)
6. Fuxman, A., Liu, L., Pistore, M., Roveri, M., Mylopoulos, J.: Specifying and Analyzing Early Requirements: Some Experimental Results. In 11th IEEE International Requirements Engineering Conference, pp. 105-114. September (1993)
7. 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), June. LNCS 4495, pp. 218-232, Springer (2007)
8. Ghanavati, S., Amyot D., and Peyton, L.: A Requirements Management Framework for Privacy Compliance. Proceeding of the 10th Workshop on Requirements Engineering (WER'07), Toronto, Canada, pp. 149-159, May (2007)
9. Giorgini, P., Kolp, M., and Mylopoulos, J. (2003). Organizational patterns for early requirements analysis. In 15th Conference on Advanced Information Systems Engineering (CAiSE*03). LNCS 2681, pp. 617-632, Springer (2003)
10. Giorgini, P., Mylopoulos, J., Nicchiarelli, E., and Sebastiani, R. (2002). Reasoning with goal models. In 21st International Conference on Conceptual Modeling (ER2002), Tampere, Finland. LNCS 2503, pp. 167-181, Springer (2002)
11. Giorgini, P., Massacci, F., Mylopoulos,J., and Zannone, N.: Requirements engineering meets trust management: Model, methodology, and reasoning. In Proceedings of the 2nd International Conference on Trust Management (iTrust 2004), LNCS 2995, pp. 176–190, Springer (2004).
12. HIPAA, The Overview, www.cms.hhs.gov/hipaaGenInfo (accessed January 2009)
13. ITU-T: User Requirements Notation (URN) – Language definition. ITU-T Recommendation Z.151 (11/08). Geneva, Switzerland, November (2008)
14. Rolland, C. Reasoning with goals to engineer requirements. In 5th International Conference on Enterprise Information Systems, Angers, France, April (2003)
15. Siena, A., Bonetti, A., and Giorgini., P.: Balanced Goalcards: Combining Balanced Scorecards and Goal Analysis. Proceedings of the Third International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2008). Funchal, Portugal, May (2008)
16. Siena, A., Maiden, N. A. M., 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 20th International Conference on Advanced Information Systems Engineering (CAiSE'08), Montpellier, France, June. LNCS 5074, pp. 182–196, Springer (2008)