Towards a Framework for Tracking Legal Compliance in Healthcare

Sepideh Ghanavati, Daniel Amyot, and Liam Peyton

SITE, University of Ottawa, Canada
{sghanava,damyot,lpeyton}@site.uottawa.ca

Abstract. Hospitals strive to improve the quality of the healthcare they provide. To achieve this, they require access to health data. These data are sensitive since they contain personal information. Governments have legislation to ensure that privacy is respected and hospitals must comply with it. Unfortunately, most of the procedures meant to control access to health information remain paper-based, making it difficult to trace. In this paper, we introduce a framework based on the User Requirements Notation that models the business processes of a hospital and links them with legislation such as the Ontario Personal Health Information Privacy Act (PHIPA). We analyze different types of links, their functionality, and usefulness in complying with privacy law. This framework will help health information custodians track compliance and indicate how their business processes can be improved.

Keywords: Business Process, Compliance, Health Information Custodian, Privacy Legislation, Requirements Engineering.

1 Introduction

Hospitals strive to improve the quality of the healthcare they provide. To achieve this, they require access to health data. These data are sensitive since they contain personal information. Disclosing this information accidentally, may affect negatively the individual's life. To prevent such situations, governments have established legislation to ensure that patient privacy is respected and hospitals, as health information custodians, must comply with it. For example, the Personal Health Information Privacy Act (PHIPA) protects electronic patient information from being disclosed to unauthorized third-parties in the Canadian province of Ontario [1]. Our objective is to provide health information custodians with tools that will allow them to protect patient data and track their compliance to legislation like PHIPA.

This paper describes a requirement management framework which connects privacy laws to business processes and helps health information custodians to ensure their business processes comply with these laws. This framework has been developed iteratively based on a case study. This framework uses the User Requirements Notation (URN) [2,3] to model both the business processes of a health information custodian and the applicable privacy legislation. Links are

J. Krogstie, A.L. Opdahl, and G. Sindre (Eds.): CAiSE 2007, LNCS 4495, pp. 218–232, 2007.

created between the two models to track the custodian's compliance to the law. To provide this traceability, we use a commercial requirements management system (Telelogic DOORS) [4] combined with an Eclipse-based URN modeling tool (jUCMNav) [5]. With these tools we are able to specify a variety of link types that connect the two models, each providing a different function. For instance, *traceability* links are used to handle compliance with the non-functional requirements defined in legal documents while *compliance* links are used to handle exceptions and constraints. Using these link types, we are able to find missing goals, special constraints, and discrepancies in the responsibilities of the various entities involved in a case study of The Ottawa Hospital (TOH).

Our technical framework will enable health information custodians to evaluate their business processes in terms of their compliance with privacy legislation. It will also allow them to make decisions about how they will remain compliant as business processes and legislation evolve over time.

2 Background and Related Work

2.1 Personal Health Information Privacy Act (PHIPA)

PHIPA [1] is legislation specific to healthcare in the Canadian province of Ontario within the framework of the federal Personal Information Protection and Electronic Documents (PIPEDA) act [6]. PIPEDA has been recognized by the European Commission as being compliant with the European Union's Data Protection [7]. In the United States, there is similar legislation for healthcare in the form of the Health Insurance Portability and Accountability Act (HIPAA) [8].

PHIPA is divided into seven parts with a total of 75 sections. It establishes a set of rules pertaining to the collection, use, and disclosure of personal health information with the goal of protecting the privacy of the individual (e.g., the patient). These rules specify that health information custodians (e.g., hospitals) obtain data with consent; that they use it only for the purposes stated; and that they do not disclose the data without the consent of the individual. The health information custodian must also provide the individual with access to his/her data with the capability to amend it if desired. Individuals must also be allowed an avenue for an independent review with respect to the handling of their personal information and remedies must be provided if it is deemed that the information was handled inappropriately.

2.2 User Requirements Notation (URN)

The User Requirements Notation is a draft ITU-T standard that combines goals and scenarios in order to help capture, model, and analyze user requirements in the early stages of development [2]. It can be applied to describe most kinds of reactive and distributed systems as well as business processes.

URN is composed of two complementary notations: *Goal-oriented Requirement Language* (GRL) and *Use Case Maps* (UCM) [9]. These notations together connect goals and business processes. GRL models business objectives,

rationales, tradeoffs, and non-functional aspects (the "why" aspects) while UCM focuses more on architectures and functional or operational aspects of business processes (the "who", "what", "where", and "when" aspects).

GRL combines a subset of the Non-Functional Requirements (NFR) [10] and the i^* [11] frameworks. The main concepts (e.g., actors, intentional elements, and links) are borrowed from i^* supplemented with the NFR framework's evaluation mechanism (i.e., qualitative labels associated to lower-level intentional elements used to compute the satisfaction degree of high-level intentional elements.) GRL's intentional elements include goals, softgoals (which can never be fully satisfied), and tasks (solutions). Such elements can contribute positively or negatively to each other and be decomposed in an AND/OR graph. In addition, they can be allocated to actors, who as a result may have conflicting concerns. See Figure 1 (left side) for an overview of the main notation elements and Figure 3 for an example.

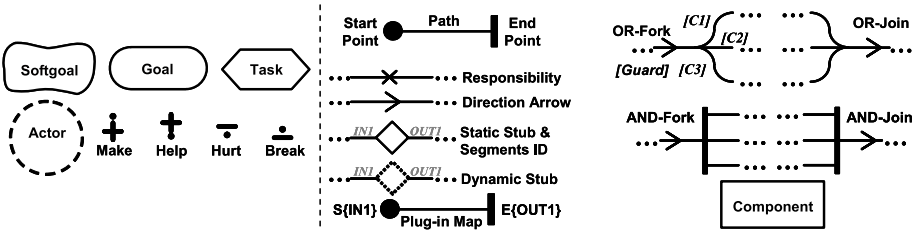


Fig. 1. Main elements of the GRL and UCM notations

The UCM notation is used to model related scenarios and use cases. As illustrated in Figure 1 (right side) and in Figure 4, scenario paths connect start points (preconditions and triggering events), end points (post-conditions and resulting events), and responsibilities. Responsibilities indicate where actions, 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. 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. The path elements (and especially responsibilities) can be allocated to components, which can represent actors, roles, software modules, sub-systems, etc. Components can also be decomposed recursively with sub-components.

2.3 URN for BPM and Requirements Management

Business Process Modeling (BPM) is used by an organization to represent its current and planned business processes as a basis for improving the mechanisms

used to achieve business goals while taking into consideration the interests of the various stakeholders [12,13]. In [3], the authors illustrate how URN can be effective in modeling business processes and goals while including stakeholders in the modeling process. GRL helps to model the risks and benefits for different alternative business processes as well as the dependencies between participants, and allow refinements of business goals into high-level tasks and/or low-level UCM responsibilities, scenarios, and plug-ins.

In [5,14], the authors have introduced a metamodel which defines URN models and combines them with external requirements documents in a Requirement Management System (RMS), namely Telelogic DOORS. We reuse and extend this approach to implement a generic framework to track compliance between two URN document-based models.

2.4 Related Work

Darimont *et al.* describe an approach where one of the main goal-oriented requirements engineering methodologies (called KAOS) is used to model regulations [15]. They explain how to incrementally transform regulation documents into three models for goals, objects, and threats while maintaining a level of traceability from the source document to the models. This method, however, does not combine the three models into one integrated model. The integration of the models would help exploit traceability in a more effective manner. A modeling language such as URN has the capacity to represent high-level goals, actors, and tasks (activities) in one model. It employs different strategies to illustrate conflicting intentions and their impact on the main high-level objectives and scenarios of the system.

He *et al.* introduce the Requirement-based Access Control Analysis and Policy Specification (ReCAPS) method [16], which integrates components of access control analysis, improves software quality, and ensures policy- and requirements-compliant systems. It emphasizes traceability and compliance between different policy levels, requirements, and system designs. ReCAPS includes a set of process descriptions and heuristics to help analysts derive and specify access control policies (ACPs) and establish traceability from source documents to these ACPs. This approach is presented in the context of the software development process and thus applies less generally than what we propose in this paper. Our method provides traceability for a compliance mechanism between business processes and legal documents, with consideration for how they evolve.

In [17], the authors apply goal-based modelling on the implementation of a financial system to ensure that it complies with Basel II regulations. In this method, the organization and its business processes are divided with respect to different organizational layers. The objectives, strategies, policies, and indicators (based on the definition of a goal model) are defined for each layer and provide a structure for the design of a regulation-compliant financial system. However, this method does not provide a traceability mechanism that highlights situations of non-compliance for the goals and business processes of the organization.

3 Compliance Framework

The framework we introduce here demonstrates how compliance can be tracked by defining and managing external links between two models: a model of the health information custodian's policies and business processes in terms of GRL and UCM notations, and a model of privacy legislation in terms of GRL notation.

As shown on the left-hand side of Figure 2, we use GRL to capture the policies of a health information custodian and UCM to represent the business processes that implement them. The figure further serves to illustrate the types of links that connect the different levels of the health information custodian model. We identify two types of links, namely:

- *Source Links*: These are the links between actual policies and procedure definitions in the original textual documents and the hospital GRL or UCM model elements.
- *Responsibility Links*: Each GRL element can be linked to one or more UCM elements. Softgoals and goals can be linked to maps of the UCM business processes that realize them while tasks and actors can be linked to UCM elements like responsibilities and agents.

On the right-hand side of Figure 2, we show how GRL is used to model privacy legislation in terms of softgoals, goals, tasks and actors. Since privacy legislation usually includes few or no operational procedures, it is usually not worth investing in UCM models for such legislation. The only link type here is:

- *Source Links*: Similar to source links for the health information custodian, these are the links between the actual legislative documents and the privacy legislation GRL elements.

After developing the health information custodian model and the privacy legislation model, we can establish links between them. Since we have two different ways of representing legal documents (textual document format, and

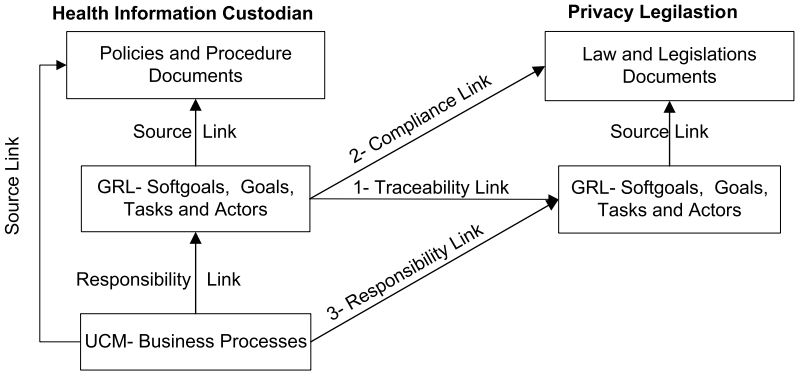


Fig. 2. Modeling compliance of health information custodian to privacy legislation

GRL model), we can construct different sets of links from these representations between the health information custodian and privacy legislation. These links can be added depending on the functionality desired. The links defined in our framework are shown in Figure 2:

1. *Traceability Links*: between health information custodian GRL elements and privacy legislation GRL elements (softgoals, goals, tasks, and actors).
2. *Compliance Links*: between health information custodian GRL elements and the actual text of the law and legislative documents.
3. *Responsibility Links*: between health information custodian UCM elements and privacy legislation GRL elements.

These links can be used to highlight the difference between what is implemented in business processes and what is required by privacy legislation. Missing and unnecessary elements in the business processes can be addressed and compliance can be tracked and managed.

4 Application to a Teaching Hospital and PHIPA

In our example, we study the business process that is in place to control access to a major teaching hospital's data warehouse in Ontario. This hospital is interested in improving the effectiveness and the efficiency of its healthcare and its support of health services research. Its plan for achieving these goals includes making its data more readily accessible to its stakeholders, including doctors, researchers, other hospitals, and patients. However, due to the existence of legislation protecting the use of health information, the hospital has established policies and heavy procedures to control the access to the data warehouse. Anyone requesting access to the data warehouse must follow this process.

4.1 Hospital Model

The hospital GRL model was derived from the hospital's data warehouse policies and guidelines document [18]. The process that controls access to the data

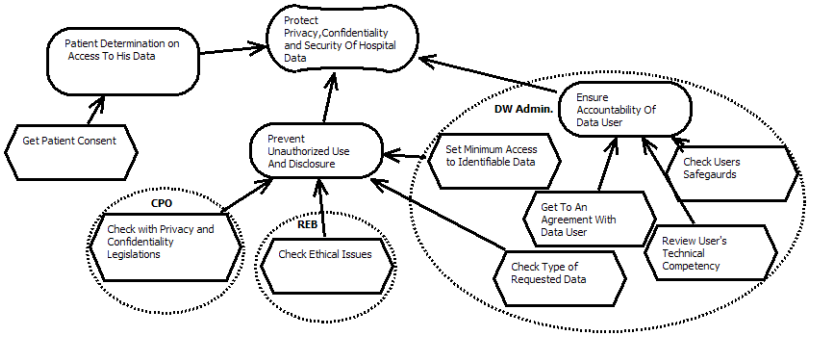
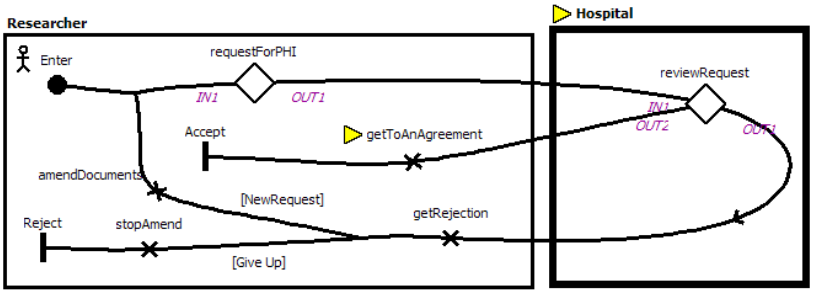
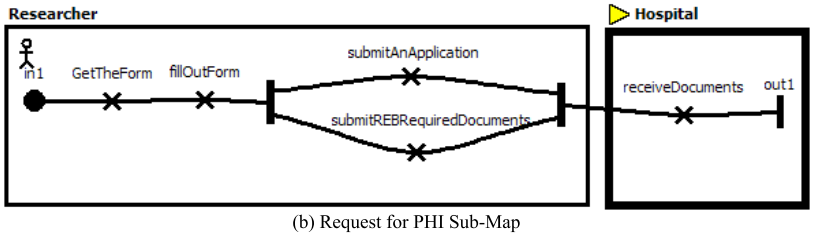


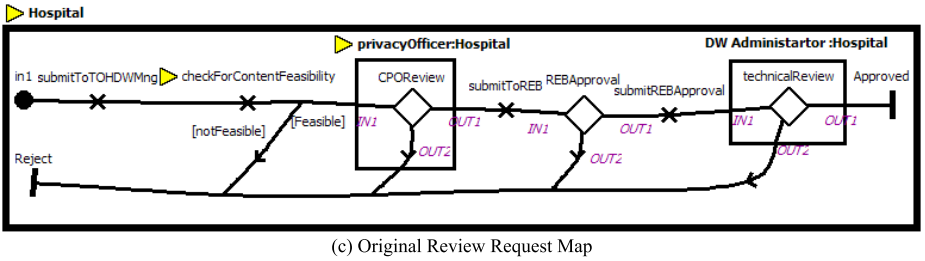
Fig. 3. Partial hospital's GRL model



(a) Top level Use Case Map



(b) Request for PHI Sub-Map



(c) Original Review Request Map

Fig. 4. Partial hospital's UCM model

warehouse is modeled with the UCM notation. We then used jUCMNav to create the GRL and UCM elements as well as the links between them. jUCMNav is an open source Eclipse-based graphical editor and analysis tool for the User Requirements Notation [5].

The hospital must ensure that stakeholders get the required information while protecting the privacy, confidentiality, and security of health data. Therefore, the partial GRL diagram of Figure 3 contains a softgoal called Protect Privacy, Confidentiality and Security of Hospital Data. Other goals contribute positively to this objective, such as Ensure Accountability of Data User, Prevent Unauthorized Use and Disclosure and Patient Determination on Access to His Data. In addition, this GRL diagram allocates the general goals and concerns to their respective actors: Research Ethic Board (REB), Data Warehouse Administrator (DW Admin), and Privacy Officer (CPO). GRL tasks are used to operationalize the parent softgoals or goals and they can correspond to responsibilities in the UCM model.

This GRL diagram illustrates some of the necessary business process scenarios and some of the activities required in the corresponding UCMs. To model how the

goal Prevent Unauthorized Use and Disclosure would be operationalized, we built a top-level UCM diagram (Figure 4(a)) and six sub-maps. This diagram shows how a researcher who needs personal health information (PHI) interacts with the hospital. This map contains Request for PHI and Review Request sub-maps, also shown in the figure. The Review Request sub-map also includes three stubs containing a Privacy Officer Review sub-map (CPO Review), a Research Ethics Board Approval sub-map (REBApproval), and a Review Request Technically sub-map (technicalReview).

Each part of these UCM diagrams potentially corresponds to a GRL element. Therefore, there are some links between them, i.e., *responsibility* links. Some of the links can be created manually inside jUCMNav (indicated by a ▷ triangle next to the label). In this example, we created links between GRL actors and UCM components, and between GRL tasks and UCM responsibilities. In Figure 4(c), the link labeled privacyOfficer:Hospital is a link from a UCM component to the GRL actor CPO in Figure 3. Also, UCM responsibility checkForContentFeasibility is linked to GRL task Check Type of Requested Data in Figure 3.

4.2 Privacy Legislation Model

The relevant sections of the PHIPA legislation were also modeled with URN. Figure 5 shows a partial GRL diagram that highlights PHIPA's major softgoal: Satisfy Privacy Regulations and Protect Confidentiality. This softgoal has many other softgoals, not shown here, that contribute to its satisfaction. Such softgoals can be broken down into goals such as Limiting the Collection of Data, Limiting the Use of Data, Secure Transfer, and Limiting the Disclosure of Data.

This GRL diagram also contains tasks that operationalize several goals. For example, for the goal Limiting the Disclosure of Data, four tasks have to be performed. One of them (Ask for REB Approval) is also decomposed into Check for Adequate Safeguards and Check Ethical Issues in Research Plan subtasks ([1], Chapter 3, Schedule A, s.44).

4.3 Model Linking

The dependencies and links that exist between PHIPA documentation, hospital documentation, GRL elements, and UCM elements were managed using Telelogic DOORS [4]. DOORS is used to collect, organize, and link requirements in a database as well as to trace, analyze, and manage changes to information in order to ensure compliance to the specified requirements and standards. jUCMNav has a filter that can be used to export GRL and UCM elements to DOORS (including internal links) so that they can be maintained [5,14]. In DOORS, we establish links between the PHIPA and hospital models and look for situations of non-compliance or any areas that require modification. In addition, we test the different types of links (described in the previous section) and determine which ones are best in terms of functionality, precision, quantity of manual links, difficulty, and completeness. A portion of the framework, along with its defined links, is illustrated in Figure 6. This figure provides a high-level overview of what

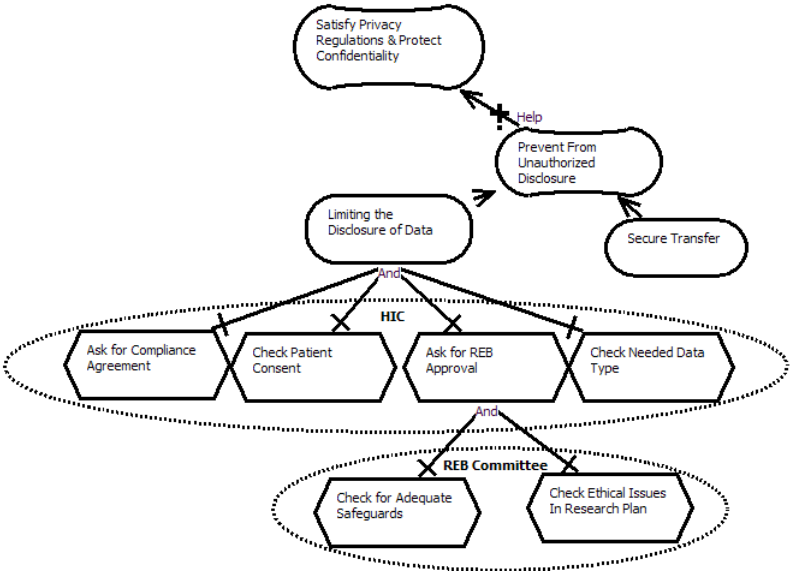


Fig. 5. Partial PHIPA GRL model

exists in DOORS and describes the different types of links that exist between elements of the hospital and PHIPA models.

After establishing manual and automatic links in DOORS, we analyze each type of link to find potential non-compliance issues. Figure 7 shows a partial overview of traceability links as they exist between the hospital GRL elements and the PHIPA GRL elements. For example, there is a link between softgoals Protect Privacy and Confidentiality of Hospital Data and Satisfy Privacy Regulations and Protect Confidentiality. We also find links between tasks Get to an Agreement with Data User and Ask for Compliance Agreement as well as between actors REB and REB Committee. These links illustrate that the hospital is trying to be compliant with PHIPA.

On the other hand, by studying these *traceability* links, it is obvious that there are some elements in PHIPA which do not have any corresponding element in the hospital model. For example, the PHIPA goal Secure Transfer is not linked to any task or goal at the hospital. This is however of critical importance to the hospital. It shows that the hospital may not comply with PHIPA thoroughly. As a result, the hospital may need to add this goal or a task to its model and ensure that processes are implemented to support it.

Moreover, a more detailed analysis of these links reveals further areas of potential non-compliance. From Figure 7, we can identify that there are some tasks, which are currently performed by a specific actor in the hospital model which have to be done by a different actor in the PHIPA model. For example, the task Check for Adequate Safeguards is handled by the REB committee but at the hospital the Data Warehouse Administrator is in charge of it. These discrepancies

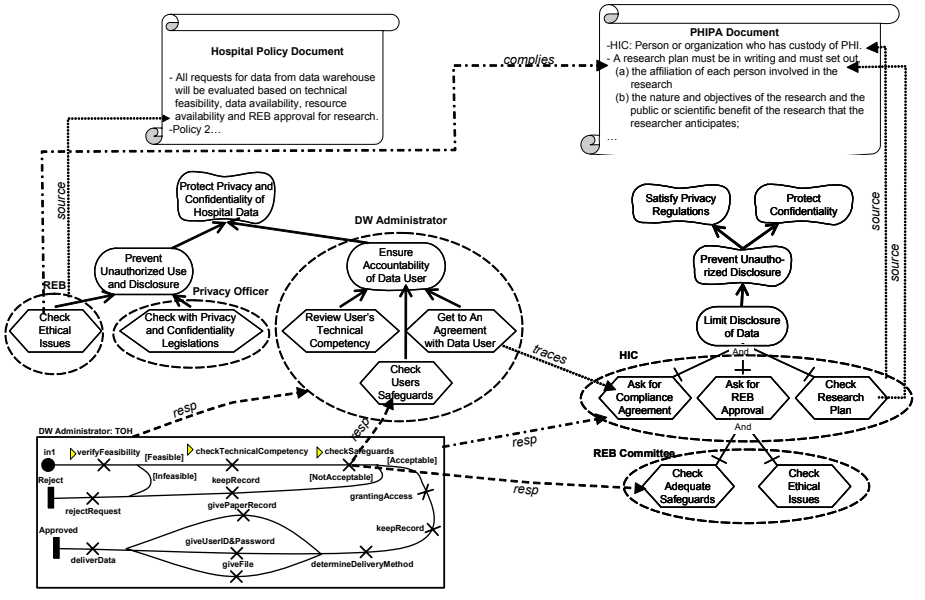


Fig. 6. Example of privacy compliance links in the hospital model

may lead to changes in the hospital model and clarification of the processes that implement the tasks.

The next links established are *compliance* links as they exist between the hospital GRL elements and the PHIPA document. This link set illustrates the details of PHIPA, the exceptions, and certain definitions that cannot be modeled using URN. An example is the goal Prevent Unauthorized Disclosure, for which the REB needs to check the ethical issues of the request. In PHIPA such a request is

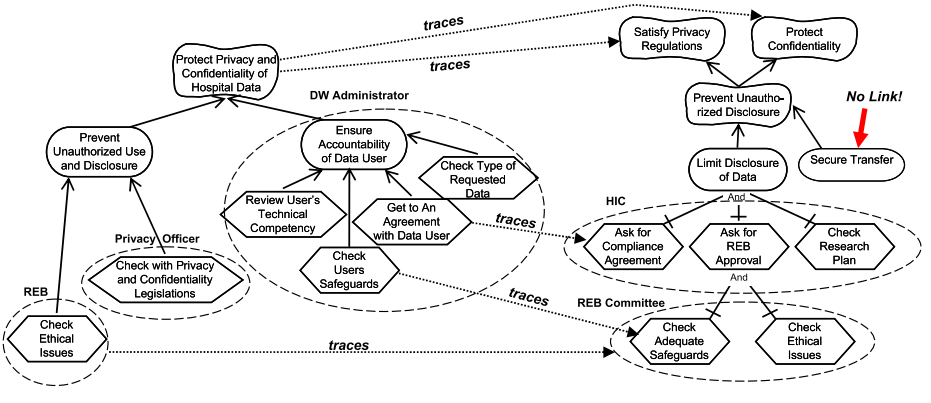


Fig. 7. Link set between hospital GRL and PHIPA GRL models

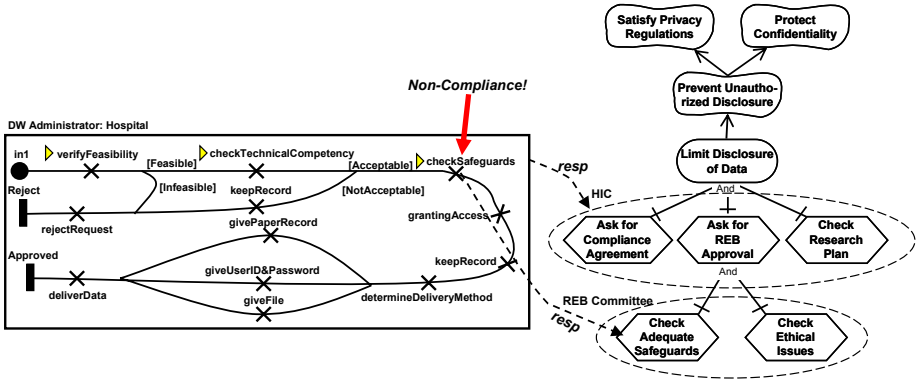


Fig. 8. Link set between hospital UCM and PHIPA GRL models

called the "Research Plan" and it has some requirements that cannot be defined with softgoals, goals, or tasks. In PHIPA, Chapter 3, Schedule A, s.44 (2), it is written that "*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.*" As a result the task Check Ethical Issues in the hospital model is linked to this text to ensure that the research plan satisfies the PHIPA requirements (Figure 6).

The last link set is concerned with *responsibility* links. These links are created between responsibilities, components, and maps in the hospital UCM model and tasks, actors, goals, and softgoals in the PHIPA GRL model. Figure 8 shows some *responsibility* links (represent as "resp") between a UCM (ReviewRequest Technically map) element and the partial PHIPA GRL model. This link type is similar to the *traceability* type in terms of utility.

As explained before, the task Check for Adequate Safeguards should be performed by the Research Ethics Board (REB) according to PHIPA. However, as seen in Figure 8, the corresponding responsibility checkSafeguards in the map ReviewRequestTechnically indicates that it is the Data Warehouse Administrator who is responsible for it. In order to address this example of non-compliance, the UCM model has to be revised and the checkSafeguards responsibility needs to be moved to a different part of the process.

5 Analysis

In this section we analyze the four types of links based on the following criteria: functionality, precision, number of manual links, difficulty, and importance of completeness.

Traceability Links: This link type is found between the HIC GRL elements and the privacy legislation GRL elements. It shows what is missing or unnecessary

in terms of the hospitals' goals and tasks (and consequently in their processes) and who is in charge of what activity. A missing softgoal, goal, or task can be a strong indication that the hospital does not completely comply with the law. Therefore, this link set is quite precise and it can help hospitals to measure their compliance very accurately. Traceability links are created manually. However, establishing this link set is not very difficult since both models are expressed at the same level of abstraction.

Compliance Links: This set differs from the first one in that instead of using GRL elements to model the privacy legislation document, we use the document itself. In practice, this set only contains those links between HIC GRL elements and the special constraints and exceptions in the text documents that cannot be modeled in the privacy GRL model. Therefore, this set is very precise and provides hospitals with additional information in order to define or improve their processes in terms of legal compliance. Creating this link set manually needs much effort but the number of manual links is fairly small and most of the links can be created through jUCMNav's auto-completion mechanism.

Responsibility Links: The main difference between these links and *traceability* links is that the hospital UCM model is linked directly to the privacy legislation GRL model. This link set is very precise since it includes fine-grained details of the business processes, so the traceability between processes and privacy legislation GRL is much easier than with the other links. However, its functionality is similar to the *traceability* links. Thus, it is often only necessary to create one of these two alternatives. In addition, as with *traceability* links, this link set needs to be complete and the number of links involved is high. However, most of these links can be created automatically by transitivity.

We evaluated each of these link sets based on the criteria mentioned above. Table 1 shows the summary of our analysis. As seen in this table, *traceability*

Table 1. Evaluation of Different Link Types

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

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

Finally, if the HIC wants to ensure that their processes comply thoroughly with the legislation and laws, it would be necessary to use *compliance* links as well. These links can be used to highlight exceptions and specific constraints that are not captured in GRL or UCM models but which are critical for ensuring compliance. They can be difficult and time consuming to define, since they require direct reference to legal text, but it is only necessary for specific critical parts of the privacy legislation documents. It is likely that a privacy expert or a lawyer would highlight relevant HIC document passages that should be linked to the privacy model.

6 Conclusions

In this paper we have presented a framework that helps health information custodians analyze and improve their business processes in order to comply with relevant privacy legislation. A case study involving a major teaching hospital in Ontario and PHIPA privacy legislation was used to illustrate the framework. The User Requirement Notation (URN) was used to model the goals and business processes related to the access of confidential information stored in a data warehouse. Links were then made between this model and a model of the PHIPA privacy legislation in a requirements management system (DOORS). Different types of links were used at different levels and their functionality and accuracy were analyzed. In doing so, discrepancies were discovered that indicated possible instances of non-compliance with PHIPA legislation that would need to be addressed.

Both privacy legislation and the business processes of health information custodians are continually evolving in the face of changing technology and greater public awareness. Therefore, we will study how changes to a section of legislation will affect the goals and processes of the organization (and vice-versa) and how our framework can help guarantee that the processes will still comply with the legislation.

Finally, modeling legislation is not a new problem and our approach could benefit from recent work in that domain. For instance, Breaux *et al.* describe how to apply semantic parameterization to HIPAA privacy rules to extract rights and obligations from HIPAA text [19]. This approach could facilitate the extraction of our privacy GRL goal model. We also expect to extract generic goal and scenario models for privacy laws that could be used as patterns to kick start this process in multiple environments (PHIPA, HIPPA, PIPEDA, U.S. Sarbanes-Oxley Act,

etc.), as was done for the software architecture domain [20]. In addition, in the privacy domain, GRL models could benefit from the privacy goal catalogues and patterns suggested in [21], which also focus on the Canadian healthcare sector. This work could accelerate the creation of the models and help determine suitable operationalizations that must be found in the related business processes. Moreover, in terms of transforming privacy policies into business process, Antón *et al.* provide a taxonomy for classifying privacy goals, and examining privacy policies in order to extract system requirements using goal-mining techniques [22]. In other words, they introduce a set of guidelines for requirement engineers and policy makers to follow when they analyze and evaluate privacy policies.

Acknowledgments. This work was supported by the Ontario Research Network for Electronic Commerce. We thank Jason Kealey and Jean-François Roy for their help with jUCMNav and Alan Forster for his insights into hospital processes. Telelogic provided us with the latest release of DOORS.

References

1. Government of Ontario: Personal health information protection act (2004) (Accessed March 2007) http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm
2. ITU-T: User Requirements Notation (URN) – language requirements and framework. ITU-T Recommendation Z.150. Geneva (February 2003)
3. Weiss, M., Amyot, D.: Business process modeling with URN. International Journal of E-Business Research 1(3), 63–90 (2005)
4. Telelogic AB: Doors. (Accessed March 2007) http://www.telelogic.com/products/doors/doors/
5. Roy, J.F., Kealey, J., Amyot, D.: Towards integrated tool support for the User Requirements Notation. In: Gotzhein, R., Reed, R. (eds.) SAM 2006. LNCS, vol. 4320, pp. 198–215. Springer, Heidelberg (2006)
6. Government of Canada: Health information custodians in the province of Ontario exemption order. (Accessed March 2007) http://canadagazette.gc.ca/partII/2005/20051214/html/sor399-e.html
7. European Union: Directive on privacy and electronic communication (2002) (Accessed March 2007) http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731 en00370047.pdf
8. US Dept. of Health and Human Services: Medical privacy - national standards to protect the privacy of personal health information. (Accessed March 2007) http://www.hhs.gov/ocr/hipaa/
9. Amyot, D.: Introduction to the User Requirements Notation: learning by example. Computer Networks 42(3), 285–301 (2003)
10. Chung, L., Nixon, B.A., Yu, E., Mylopoulos, J.: Formalizing Functional Requirements in Software Engineering. Kluwer Academic, Dordrecht, USA (2000)
11. Yu, E.: Towards modelling and reasoning support for early-phase requirements engineering. In: RE'97. Proc. 3rd IEEE Int. Symp. on Requirements Engineering, pp. 226–235. IEEE Computer Society Press, Los Alamitos (1997)

12. Caetano, A., Silva, A.R., Tribolet, J.: Using roles and business objects to model and understand business processes. In: SAC 2005. LNCS, ACM Press, New York, USA (2005)
13. Staccini, P., Joubert, M., Quaranta, J.F., Fieschi, D., Fieschi, M.: Modelling healthcare processes for eliciting user requirements: a way to link a quality paradigm and clinical information system design. International Journal of Medical Informatics 64(2-3), 129–142 (2001)
14. Kealey, J., Kim, Y., Amyot, D., Mussbacher, G.: Integrating an Eclipse-based scenario modeling environment with a requirements management system. In: CCECE06: IEEE Canadian Conf. on Electrical and Computer Engineering, Ottawa, Canada, pp.2432–2435 (2006)
15. Darimont, R., Lemoine, M.: Goal-oriented analysis of regulations. In: REMO2V06: Int. Workshop on Regulations Modelling and their Verification & Validation, Luxemburg June 2006 (2006)
16. He, Q., Otto, P., Antón, A.I., Jones, L.: Ensuring compliance between policies, requirements and software design: A case study. In: WIA 2006. Fourth IEEE Int. Workshop on Information Assurance, pp. 79–92. IEEE Computer Society Press, Washington, USA (2006)
17. Rifaut, A., Feltus, C.: Improving operational risk management systems by formalizing the Basel II regulation with goal models and the ISO/IEC 15504 approach. In: REMO2V06: Int. Workshop on Regulations Modelling and their Verification & Validation, Luxemburg (2006)
18. Fairfield, D.: The Ottawa Hospital data warehouse - governance and operation procedures - phase 1 research. Technical report, The Ottawa Hospital (2004)
19. Breaux, T.D., Vail, M.W., Antón, A.I.: Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In: RE'06: Proc. 14th Int. Conf. on Requirements Engineering, pp. 46–55. IEEE Computer Society Press, Washington, USA (2006)
20. Amyot, D., Mussbacher, G., Weiss, M.: Formalizing patterns with the User Requirements Notation. In: Taibi, T. (ed.) Design Pattern Formalization Techniques, Idea Group Publishing, Hershey, USA (2007)
21. Webster, I., Ivanova, V., Cysneiros, L.M.: Reusable knowledge for achieving privacy: A canadian health information technologies perspective. In: WER'05: Workshop em Engenharia de Requisitos, pp. 112–122 (2005)
22. Antón, A.I., Earp, J.B., Reese, A.: Analyzing website privacy requirements using a privacy goal taxonomy. In: RE'02: Proc. 10th Int. Conf. on Requirements Engineering, pp. 23–31. IEEE Computer Society Press, Washington, USA (2002)