A Requirements Management Framework for Privacy Compliance

Sepideh Ghanavati, Daniel Amyot, and Liam Peyton
SITE, University of Ottawa, Canada
{sghanava, damyot, lpeyton}@site.uottawa.ca

Abstract

Compliance with privacy legislation is a primary concern for health care institutions that are building information systems support for their business processes. This paper describes a requirements management framework that enables health information custodians (HIC) to document and track compliance with privacy legislation. A metamodel is defined for our framework to define compliance tracking links between separate User Requirements Notation models of the HIC and privacy legislation. Using examples from a case study at a major teaching hospital, we show how this framework can be used to manage change and ensure compliance when privacy legislation is amended or the business processes evolved.

1. Introduction

Compliance with privacy legislation is a primary concern for health care institutions that are building information systems support for their business processes. This paper describes a requirements management framework that enables health information custodians (HIC) to document and track compliance with privacy legislation as the legislation and hospital business processes evolve. The User Requirements Notation (URN) [1][11] is used to create separate models for hospital business processes and for privacy legislation in terms of goals, tasks, actors and responsibilities. Compliance is described by a metamodel that defines links between privacy legislation and hospital business processes as well as links between URN model elements and the source clauses of documents for privacy legislation and hospital policy. The URN models are created using an Eclipse-based URN modeling tool and then exported to a requirements management system. Internal link models are transferred automatically. Some inter-model links are created manually whereas others are inferred automatically. Using examples from a case study at a major teaching hospital, we show how this framework can be used to manage change and ensure compliance when privacy laws are amended or the hospital business processes and systems evolve.

2. Background

The case study was done at a major teaching hospital in Ontario, Canada, where the applicable privacy legislation is the Personal Health Information Privacy Act (PHIPA) [8]. In this section we describe this act in terms of the challenges health information custodians face in achieving compliance with it. We also discuss the modeling notation used in our work: User Requirements Notation (URN).

2.1. Personal Health Information Privacy Act (PHIPA)

PHIPA specifies the legal responsibilities of health information custodians (HIC) in terms of how they are to handle personal health information (PHI). This act was passed by the Province of Ontario in 2004. PHIPA aims to protect privacy and confidentiality of personal health information while facilitating the healthcare provision by establishing a set of rules for the collection, use and disclosure of that information [8]. 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. In addition, PHIPA asks health information custodians to provide the individual the right to access their data and let them amend it. 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.

PHIPA is legislation specific to healthcare in Ontario, but it exists within the framework of the federal Personal Information Protection and Electronic Documents (PIPEDA) act [7]. PIPEDA has been recognized by the European Commission as being compliant with the European Union's Prime Directive on Privacy and Electronic Communication [5]. In the USA, there is similar legislation for healthcare in the form of the Health Insurance Portability and Accountability Act (HIPAA) [16].

PHIPA, like all legislation, is open to change. Since its introduction, PHIPA has been amended 5 times: 2005, c. 25, s. 35; 2006, c. 4, s. 51; 2006, c. 17, s. 253; 2006, c. 21, Sched. C, s. 128; and 2006, c. 34, Sched. C, s. 26. These changes underline the need for a framework to manage and track compliance on an ongoing basis.

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 design [1][11]. It can be applied to describe most kinds of reactive and distributed systems as well as business processes. URN is suitable for applications ranging from goal modeling and user requirements to high-level design.

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

GRL is composed of concepts such as goals, softgoals (which can never be fully satisfied), and tasks (solutions) which collectively are called intentional elements. Such elements can contribute positively or negatively to each other in an AND/OR graph. In addition, they can be associated to actors, who may have conflicting concerns. See [1] for an overview of the notation.

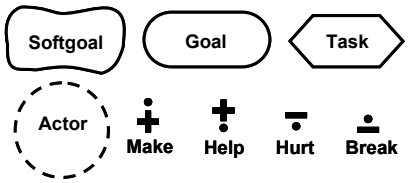

Figure 1 - Subset of GRL Notation

UCM is used to model business processes and system behavior in terms of related scenarios and use cases. As illustrated in Figure 2, 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 (using AND-forks and AND-joins) or as alternatives (with guarded OR-fork and OR-join).

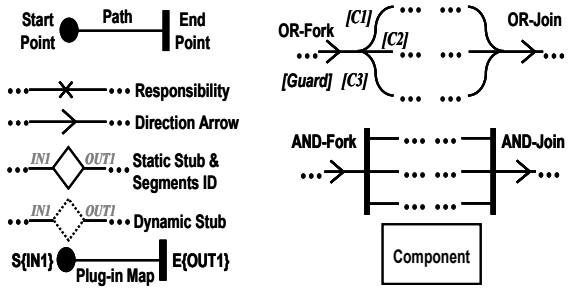

Figure 2- Subset of UCM Notation

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. 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. More details on URN (GRL and UCM) are provided in [1].

2.3. Tool Support

URN models (GRL and UCM) are built using the Eclipse-based jUCMNav tool [12]. jUCMNav supports the creation of URN models that include many GRL and UCM diagrams, as well as links between various modeling elements. jUCMNav also supports the export of URN models to Telelogic DOORS [15], a requirements management system, which is used to link the diagrams to other documents and requirements (e.g., privacy legislations and hospital policy) . In our approach, we will also use DOORS to track compliance between models of the hospital business processes and models of the legislation.

2.4 Related Work

Applying requirements engineering concepts to model traceability between textual documents, goals, and business models has been explored on several occasions.

Rifaut *et al.* [13] apply a goal-oriented requirements engineering (GORE) methodology to a financial system in order to ensure compliance between this system and Basel II regulations. With respect to the different organizational layers, the organization and its business processes are divided and their objectives, strategies, policies, and indicators are defined. This method provides a framework for establishing a regulation-compliant financial system, but it lacks a traceability mechanism to help highlight the instances of non-compliance for the organization's goals and business processes.

In[4], the authors use another goal-oriented requirements engineering methodology, KAOS, to model regulations. Following this method, regulation documents are transformed incrementally into three models for goals, objects, and threats while maintaining traceability from the source document to the target models. Since the three models are treated separately, however, it lacks integrity among the models and as a result traceability is less efficient. On the other hand, GRL, the goal modeling language we use in this paper, is able to provide a model which includes high-level goals, actors, and tasks (activities).

The Requirement-based Access Control Analysis and Policy Specification (ReCAPS) method, introduced in [10], integrates access control analysis components and ensures that systems are compliant with both policies and requirements. This method emphasizes compliance between different levels of policy, requirements and system design. Providing a set of process descriptions and heuristics, this method helps analysts specify access control policies (ACPs). This method also includes a mechanism for traceability that connects source documents to ACPs and helps to track non-compliance between policies, system requirements and software design. However, this method is only applied to the software development process and is not as general as the method we introduce in this paper.

3. Framework Overview

A high-level overview of our requirements management framework for privacy compliance is given in Figure 3. Two URN models are created. One captures the essence of the privacy legislation with a goal model. This model is independent of the organizations that desire to comply with it and, given the scarcity of operational details in such legislation, it does not prescribe a business process. The other URN model includes a GRL view capturing the goals of the Health Information Custodian's policies and procedures, and a UCM view describing the associated business process in place.

Manual links are also added (using DOORS and jUCMNav) between each of these two URN models and their source documents. On the left side of Figure 3, we have the requirements of the HIC described in terms of "source" links from policies and procedure documents to GRL elements (Goals, Tasks, and Actors) and UCM elements (Business Processes). We also make use of "responsibility" links between the GRL and UCM elements (i.e. goals, actors and tasks in GRL are connected to the UCM maps, components, and responsibilities via the internal links called "responsibility" links.) On the right hand side, we have the requirements of privacy legislation in terms of "source" links from the law and related legislative documents to the corresponding GRL elements. More details on how policies, procedures and laws are encoded as goals and scenarios can be found in [3][6].

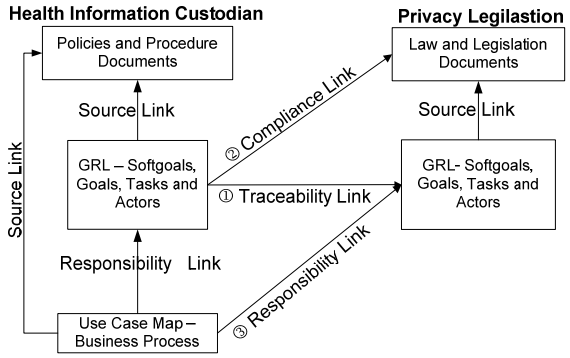

Figure 3- Requirements Management Framework

To establish and track compliance of the HIC with privacy legislation, three link sets have been identified:

1. *Traceability Links* are links between GRL elements that model the health information custodian and GRL elements that model privacy legislation. These links are created manually but this is usually not difficult because the two models are expressed at similar levels of abstraction and use similar concepts.

2. *Compliance Links* are links between GRL elements that model the health information custodian and the actual text of the law and legislative documents. Some of these links can be created manually while others can be inferred from previously created links, by transitivity.
3. *Responsibility Links* are links between UCM elements that model the health information custodian and GRL elements that the model privacy legislation. Again, some of there links are manual whereas others are automatic.

Traceability links are used to trace, at a high level, the intentional elements and actors identified in privacy legislation with the ones related to business processes at the HIC.

Compliance links are useful to highlight exceptions and additional descriptions in the legislation that are not easily communicated in diagrams. Therefore, they are very precise and provide additional information about requirements in laws.

Responsibility links are very similar to traceability links but more directly link the detailed scenarios and business processes to tasks and actors that model privacy legislation.

4. Framework Metamodel

Mussbacher and Roy have defined a metamodel for representing URN models in DOORS, which is now supported in jUCMNav [12][14]. Using *DOORS eXtension Language* (DXL) scripts and custom libraries, the tool exports various DOORS modules that contain UCM diagrams, GRL diagrams, requirements objects (e.g., actors, intentional elements, responsibilities, components, stubs) with their attributes, and many links describing internal or user-defined relationships between URN elements. This provides a view of the URN model that is useful for creating links from/to external requirements and monitoring them as requirements and models evolve. The export mechanism also offers predefined views for monitoring changes.

Also included is an *auto-link mechanism* (in DXL) that takes advantage of the internal links automatically created in the UCM model in order to automatically generate new links from manually created links, by transitivity. This helps minimizing the numbers of links to be input manually. Having direct links created in such a way also enables analysts to use basic DOORS features for performing traceability and impact analysis as models evolve.

In our approach, we use and extend this metamodel in order to implement the generic framework presented in Figure 3. This new metamodel is summarized in Figure 4. As explained in [12][14], the only URN model elements exported are those likely to be useful from a requirements linking and management perspective. Importing all links into a requirements management system would lead to performance degradation and usability issues because of too many unnecessary details. In this class diagram (where attributes and less relevant classes and associations are hidden), shaded classes are separate DOORS formal modules, and named associations are link modules. Note that although some associations have directions, corresponding link instances can be navigated in both ways in DOORS.

The legislation model (bottom part of Figure 4) includes the privacy legislation documents and GRL model introduced in Figure 3. The source document, which defines *clause* and *definition* objects, is imported as is into DOORS. Once a GRL model has been created out of it, *source* links from the *intentional elements* and *actors* are manually added. Note that this needs to be done only once for each law. Also, with a requirements management system such as DOORS, missing links can easily be identified when there is no mapping for a requirements object (e.g., a GRL element) to the source document. This is actually the case for most modules in our system.

At the top of Figure 4, the HIC model contains GRL diagrams (goals) and UCM maps (business processes). Many internal links are generated automatically from the URN model. The source policy and procedure documents are again imported as is and linked manually. Responsibility links (resp) from UCM elements to GRL elements are created manually using jUCMNav (also transferred to DOORS).

Once both the HIC model and the Legislation model are available, traceability links ① between the two GRL models can be added using DOORS. We establish traceability links from the *actors* and *intentional elements* of the health information custodian model to the *actors* and *intentional elements* of the privacy legislation model. Then, compliance ② and responsibility ③ links can be set up manually or by auto-completion (currently only available for the UCM part, but the GRL part will be added very soon). Compliance links are set up between the *actors* and *intentional elements* of the health information custodian model to the *definitions* and *clauses* of the privacy legislation. Responsibility links are built from the *maps, responsibilities*, and *components* to the *intentional elements* and *actors* of privacy legislations.

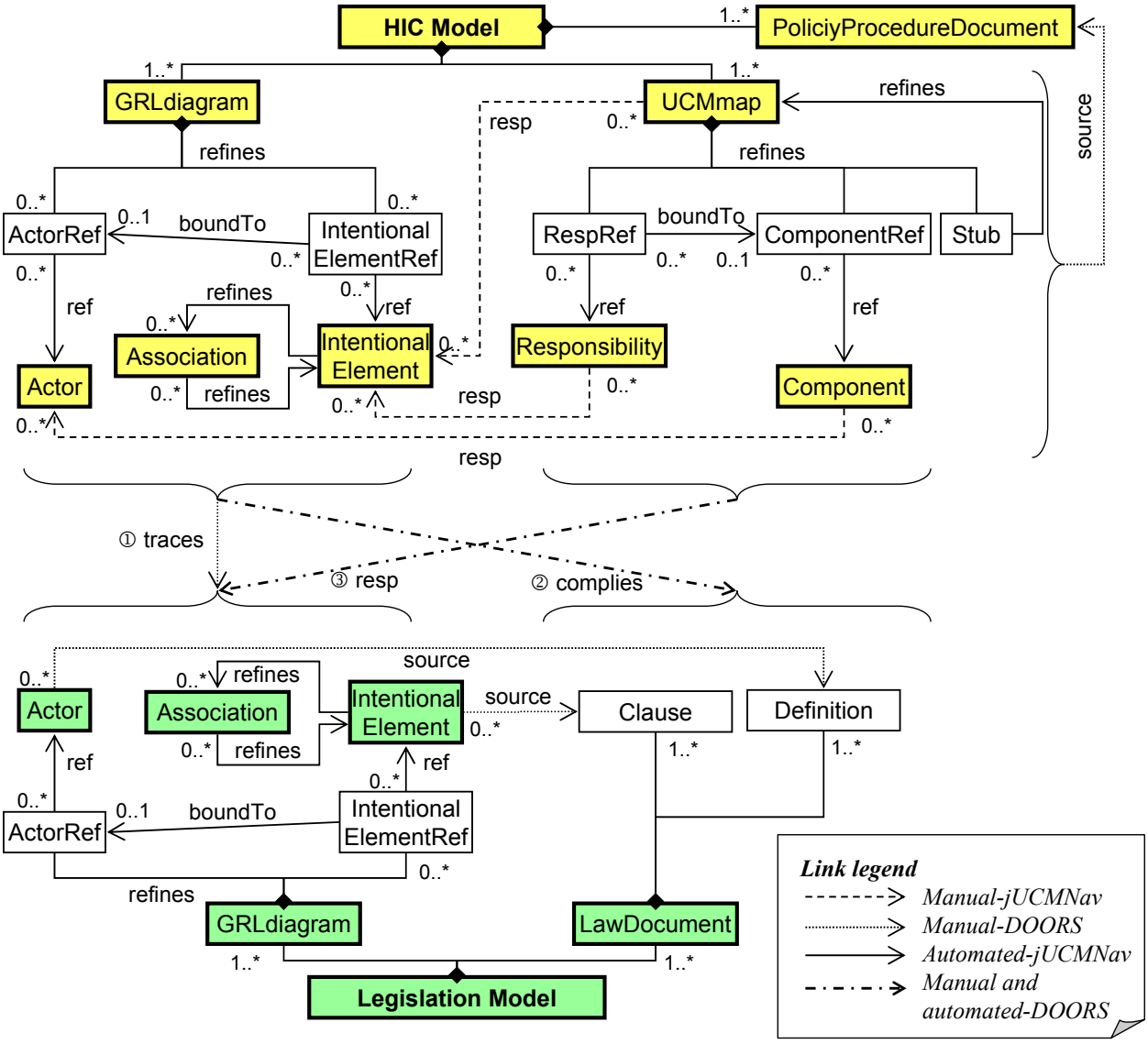

Figure 4- Framework Metamodel in DOORS

Such a metamodel helps us determine which links need to be created manually and which ones can be inferred automatically. If the creation of a link can be automated, then this will help reduce the amount of effort required to implement the compliance framework. On the other hand, inferring too many links will make the tool less usable, especially during evolution (one change might lead to a situation where the entire model needs to be revisited, which is not helpful). Balancing the need for minimizing the manual effort while ensuring all necessary links are present and useless links are absent, is still a challenge we are facing.

Figure 5 illustrates how this framework metamodel can be instantiated in the context of a hospital business process that has to comply with PHIPA. In this excerpt of a larger model, we can observe part of the HIC policy document, its goal model, and the corresponding business process. On the right side, the PHIPA legislation document is modeled with GRL. URN internal links (*ref*, *refines*, *boundTo*, etc.) are not shown here; they correspond to the regular relationships illustrated by the diagrams themselves. However, one can observe examples of several *source* and *traces* links, manually created in DOORS, and *resp* links, manually created between UCM and GRL views in jUCMNav. The *complies* links and the other *resp* links can actually be inferred automatically by transitivity, but some could be input manually as well.

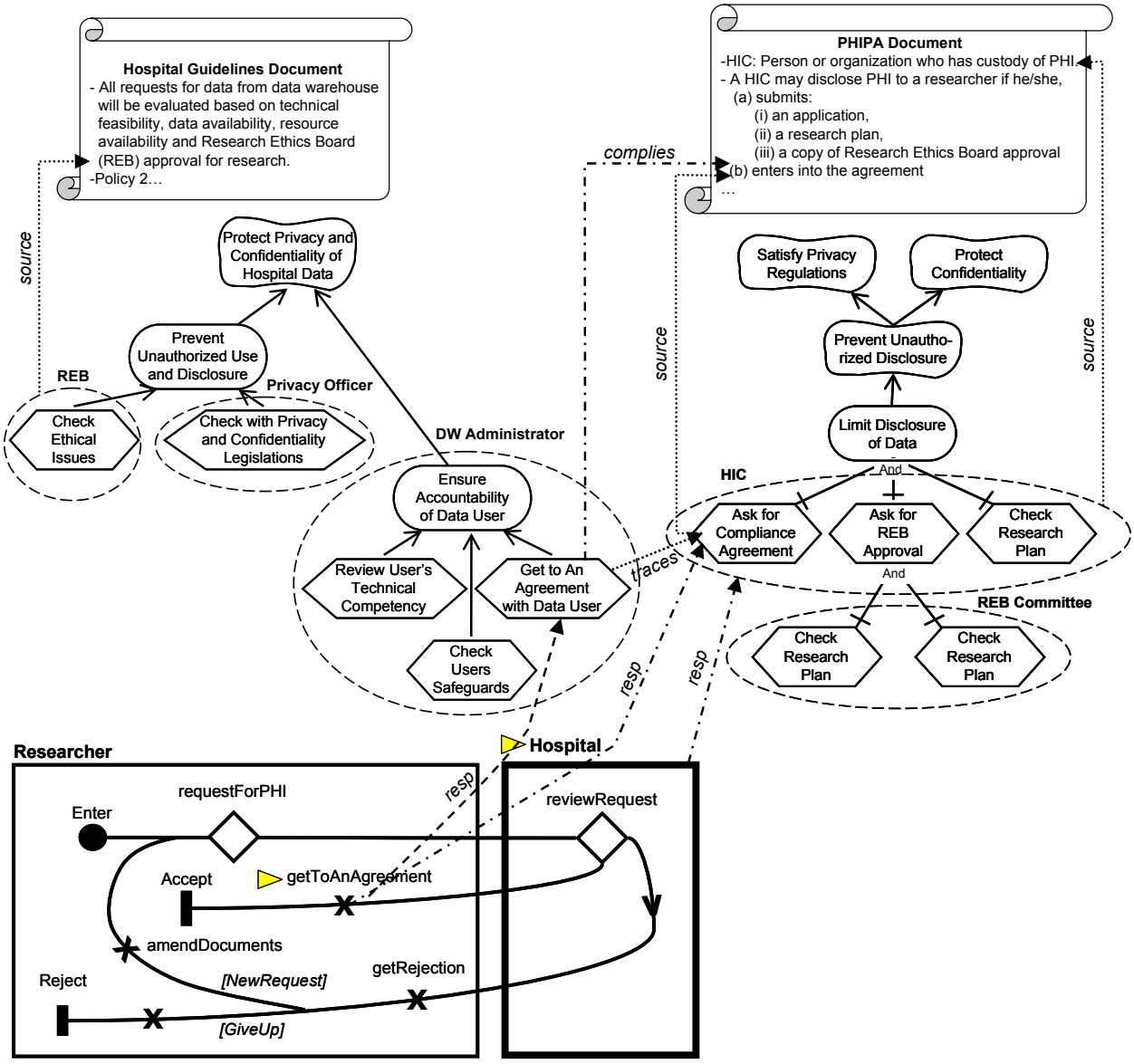

Figure 5- Example of Privacy Compliance Links in a Hospital (Excerpt)

In the next section, we will show how this meta-model also enables one to manage and maintain compliance in the face of amendments to the privacy legislation or in the face of changes to the business processes at the health information custodian.

5. Managing Evolving Privacy Legislation

In this section, we look at the different scenarios by which legislative documents can be amended. The relevant cases to consider are:

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

The impact of these changes on the HIC's business processes and goals can be tracked through the link sets identified in the previous section. Note that deleting an existing clause without links to HIC require-

ments will not impact the health information custodian. As shown in Figure 3, when legislative or other legal documents (source documents) are modified, this will directly affect the source links targeting these documents and the compliance links of the health information custodian GRL. In turn, the modified legislation GRL may affect the traceability and responsibility links along with the corresponding source elements in the HIC GRL or UCM.

Here, we explain the impact of each of the above scenarios and then we give an example for one of the cases.

5.1. Addition of a New Clause

When a new clause is added to the legislation, one of three cases applies:

I. **It refers to an existing actor, softgoal, goal, or task.** In this case, the clause can act as an additional description, an extension or exception for the existing actor, or intentional element. Therefore, this new clause must be linked to the privacy legislation GRL. In doing this, the GRL itself will not change. With the addition of a compliance link, it may be possible to indicate the elements of the HIC GRL that are likely to be affected by the new clause. By adding a traceability link, the impact of the new clause on the HIC GRL is traced. A responsibility link will model the impact of the added clause on the UCM.

II. **It introduces a new actor, softgoal, goal or task.** This case is similar to the initial situation where a hospital derives the link sets between two models for the first time. The legislation GRL and the health information custodian GRL will change and new elements will be added to both GRL models. In addition, the existing UCM business process may need to be modified to incorporate these new elements. Moreover, the link sets need to be updated and adding new links may be required.

III. **It is irrelevant.** The added clause does not refer to actors, softgoals, goals and tasks of the business processes.

5.2. Modify a Clause with Links

If a clause is modified, the legislation GRL must be changed. The effect of this change on the legislation GRL can be traced by a *source link,* and also to the health information custodian GRL via a *compliance link.* This modification can be made to either actors or intentional elements. Modification of the actors usually implies a change to the definition of the actor, whereas a modification of an intentional element means an update in responsibilities of the business process.

When an intentional element changes, this effect can be traced by either *traceability links* or *responsibility links*. If a traceability link is used, the part of the HIC GRL that must be considered will be highlighted. If the HIC GRL needs to be modified, it will affect the UCM. The affected part of the UCM will be highlighted by an internal *responsibility link*.

5.3. Delete a Clause with Links

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

Clauses and their corresponding GRL elements also have links to the health information custodian models. As a result, when a clause is deleted the impact is highlighted in the HIC GRL and UCM. This may in turn lead to updates of the corresponding UCM (functionalities might not be necessary any longer, or fewer constraints may lead to new optimization opportunities). After, the impact is confirmed and the GRL and UCM changes are performed, these links can also be deleted.

5.4. Modify a Clause without Links

This case is largely identical to Case 5.1 with the exception that for this case the modified clause is more likely to be irrelevant to the task of privacy compliance tracking. However, in terms of having impact on the health information custodian, the modification can be handled as for Case 5.1.

5.5. Case Study Example

In our case study, we modeled the compliance of business processes at a major teaching hospital in Ontario (Canada) with PHIPA, which is the relevant privacy legislation. As mentioned in section 2.1, PHIPA has evolved over the years and now contains several amendments. In the latest PHIPA amendment [9], a new extension clause was added to an existing clause. More specifically, the clause *Requirements for Research Plan ,* O. Reg. 329/04, s. 16 was added to the *Research Plan,* 2004, c. 3, Sched. A, s.44 (2) clause. Figure 6 shows this change in a privacy legislation document with a bold italic font.

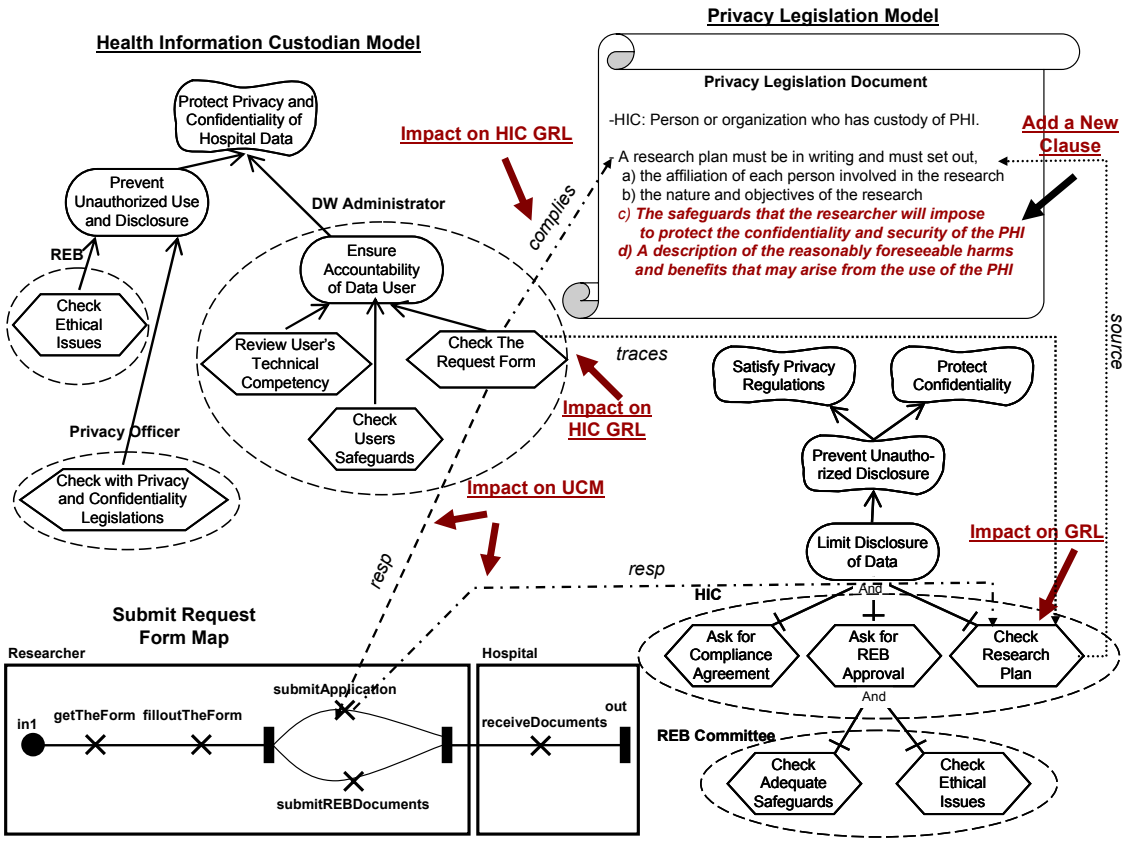

Figure 6 - New Clause Added

Since this new clause refers to an existing intentional element in the privacy legislation GRL, namely, *Check Research Plan*, and it relates to the *Research Plan* clause in PHIPA, it is only necessary to establish an internal source link between the two elements. However, this intentional element is linked to the HIC GRL and UCM via traceability and responsibility links. Therefore, with the help of these links, we can trace that the *Researcher-Root* map and the responsibility *getToAnAgreement* (with the researcher) have to be checked. The indication of this impact is illustrated in Figure 6.

6. Managing Evolving Business Processes

The business processes of a HIC are also susceptible to change. As they evolve, the HIC needs to verify whether their business processes still comply with privacy laws and legislation. As illustrated in Figure 3, when a business process (UCM) changes, it may directly impact the responsibility links to the health information custodian GRL or to the legislation GRL. These, in turn, can also affect the source links, compliance links and traceability links. The impact on the above links has to be carefully managed in order to ensure that compliance is still maintained.

When business processes change, one of the following three cases needs to be addressed:

1. An existing process UCM diagram is modified
2. A new process UCM diagram is added
3. An existing process UCM diagram is removed

Next, we briefly explain each of these cases.

6.1. Modify an Existing Process

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

I. The existing process has links to its GRL and legislation GRL. In this case, the compliance can be quickly verified using the various kinds of links, i.e., responsibility links, traceability links, or compliance links.

II. The existing process does not have links to its GRL and legislation GRL. In this case, it may be necessary to check whether or not this modification can be affected by any part of the legislation. In the

unlikely event it relates to the legislation, it then becomes necessary to add the necessary links and then use them to verify whether the process is still compliant with the law or not.

6.2. Add a New Process or Element

When a new process is added to the model, we need to consider the laws carefully in order to determine whether or not the new process needs links to the legislation. If required, the links are added and then used to verify the compliance. Otherwise, the new process is not relevant to the privacy issues.

6.3. Remove Part of a Process

When a business process is removed, it is necessary to also remove all of its out-going links. If it is connected to the privacy legislation GRL model by way of responsibility links, then the removal might result in an incomplete and non-compliant process. If no link is present, then this part can safely be removed from a privacy standpoint.

6.4. Example

Here we give a simple example from our case study that illustrates how the framework can be effective in the face of process change. In the *review request technically* UCM, we chose the responsibility *check safeguards* and made it more specific to *check physical safeguards*. This change is illustrated in DOORS by the display of a (red) change bar, as shown in Figure 7.

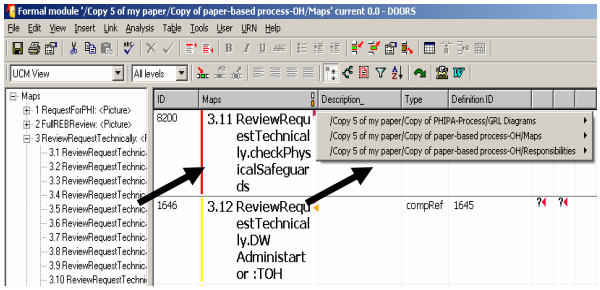

Figure 7- A Responsibility Changed

As indicated by the arrows, this responsibility has some links to HIC GRL intentional elements and privacy legislation GRL intentional elements. Therefore, the related legislation GRL intentional element will be flagged as suspect links (with the "?◄" symbol in DOORS, see Figure 8) which indicate that attention must be paid to these elements for reassessing compliance. Suspect links are easily filtered and emphasized using custom-built views in our DXL library.

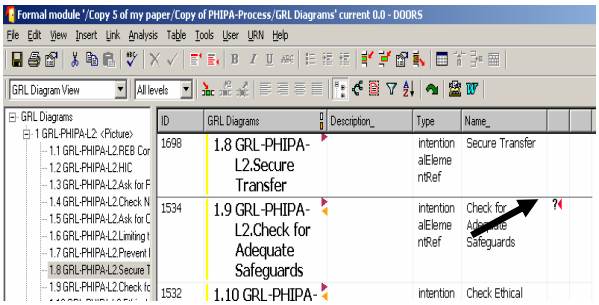

Figure 8- Related PHIPA element

Finally, through the *source link,* the related PHIPA rule can be traced. See Figure 9 for the traceability effect. We get to the intentional element *check for adequate safeguards* via the traceability or responsibility links when we check the legislation GRL. This intentional element does not restrict itself to any specific safeguard and therefore, it means the Research Ethic Board needs to check all kinds of safeguards and not only physical safeguards. As a result, the modification would result in non-compliance with PHIPA.

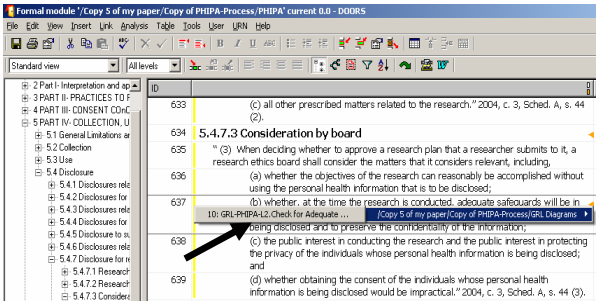

Figure 9- PHIPA Rule related to the changed responsibility

7. Analysis of the Response to Change

In the previous sections, we described how this framework helps a hospital to not only ensure that their business processes comply with privacy legislation, but also to respond to change and remain compliant. Our framework is able to handle the impact of most types of changes and helps to precisely determine whether compliance to legislation is maintained in the face of changes. With the links provided in this framework, we can track the effect of changes easily in situations where part of the legislation or the business processes is modified. However, when a new clause or process is added or an existing clause or process not previously

linked to the model is modified, it may be required to add some new links to the system. Nevertheless, this can be handled with little effort. For instance, if a completely new clause is added, the legislation GRL will be updated as well. This new element in GRL can impose a new element on the hospital GRL. Therefore, the traceability link will be set up manually quite easily. Compliance links can be established automatically right after, and then it is only required to determine what kind of change (if any) is needed for the business process to satisfy this new clause. Furthermore, another important benefit of this framework is observed when part of a business process is removed. In this case, the existing links between the HIC and legislation models can alert decision-makers of non-compliance.

The amount of effort required to establish links from scratch depends on the types of link. As mentioned in section 3, traceability and responsibility links are very precise and they need to be complete. Traceability links have to be established manually but this does not require a considerable amount of effort since such links are created between two GRL models at the same levels of abstraction. A large number of responsibility links will be set up automatically and only a few will require manual intervention. Compliance links are less difficult to define and do not need to be complete. Hence, most of these links will be created automatically.

8. Conclusions and Future Work

In this paper, we presented a requirement management framework which aids hospitals in managing their compliance with privacy law. It enables them to characterize and track the changes that must be made in order to maintain compliance when either legislation is amended or when business processes evolve. This framework contains links between the URN model for a health information custodian, and the URN model for the applicable privacy legislation. jUCMNav was the tool for creating and maintaining URN models as well as for generating links between GRL and UCM views. These models, together with the legislation documents and HIC policies, were exported to a requirement management system, Telelogic DOORS. Additional inter-model links between them were established manually or inferred automatically. The case study presented in this paper illustrates how this framework can be used in practice. As a result of our research, we found this framework to be a useful analysis and design tool, suitable for assessing and maintaining privacy compliance at a major Canadian hospital.

The next step for our work will be to extend our framework to handle multiple legislative which impose additional constraints and could, in some cases, contradict each other. Another issue is that health information custodians have other types of policy and procedure documents to consider, such as collective agreements and internal policies, that can also include conflicting goals. Handling these documents along with their impact on business processes when they change can be challenging.

Finally, modeling legislation is not a new problem and our approach could benefit from recent work in this domain. For instance, *Breaux et al.* describe how to apply semantic parameterization to HIPAA privacy rules to extract rights and obligations from HIPAA text [1]. This could help modeling legislation and policies in GRL. In the privacy domain, GRL models could also benefit from the privacy goal catalogues and patterns suggested in [17], which also focus on the Canadian health care 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 [2]. In other words, they introduce a set of guidelines for requirement engineers and policy makers to follow when they analyze and evaluate privacy policies. These guidelines are designed to help those responsible for the development of business processes to make sure that their organization is able to comply with all applicable privacy policies, and hence we could take advantage of some of these ideas in our future work.

Acknowledgments. This work was supported by the Ontario Research Network on Electronic Commerce. We thank Telelogic for making DOORS available to us, as well as J. Kealey, J.-F. Roy, and G. Mussbacher for their help with jUCMNav.

References

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

[2] Antón, A. I.; Earp, J. B. and Reese, A.: Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy. *10th IEEE Joint International Requirements Engineering Conference*, IEEE CS Press, 23–31, 2002.

[3] Breaux, T. D., Vail, M. V., and Antón, A.I.: Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. *14th IEEE Requirements Engineering Conference*, Minneapolis, USA, 46–55, 2006.

[4] Darimont , R., Lemoine, M.: Goal-oriented Analysis of Regulations, *International Workshop on Regulations Modelling and their Verification & Validation (REMO2V06)*, Luxemburg, 2006.

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

[6] Ghanavati, S., Amyot, D., and Peyton, L.: Towards a Framework for Tracking Legal Compliance in Healthcare. *19th International Conference on Advanced Information Systems Engineering (CAiSE'07)*, Trondheim, Norway, 2007.

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

[8] Government of Ontario: *Personal Health Information Protection Act, 2004*, http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/0 4p03_e.htm, accessed March, 2007.

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

[10] He, Q., Otto, P., Antón, A., and Jones, L.: Ensuring Compliance between Policies, Requirements and Software Design: A Case Study. *4th IEEE International Workshop on Information Assurance (IWIA'06)*, Royal Holloway, UK, 2006

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

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

[13] Rifaut, A, and Feltus, C.: Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach. *International Workshop on Regulations Modelling and their Verification & Validation (REMO2V06)*, Luxemburg, 2006.

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

[15] Telelogic AB: DOORS 8.1. http://www.telelogic.com/products/doors/doors/. Accessed March 2007.

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

[17] Webster, I., Ivanova, V., and Cysneiros, L.M.: Reusable Knowledge for Achieving Privacy: A Canadian Health Information Technologies Perspective. *Proc. of VIII Workshop in Requirements Engineering (WER'05)*, Porto, Portugal, 112–122, 2005.