Aligning Requirements with HIPAA in the iTrust System

Aaron K. Massey[1], Paul N. Otto[1,2], Annie I. Antón[1]
Department of Computer Science, North Carolina State University[1]
School of Law, Duke University[2]
{akmassey, pnotto, aianton}@ncsu.edu

ABSTRACT

We describe a case study in which we evaluated an open-source Electronic Health Record (EHR) system's requirements for compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA). Our findings suggest that legal compliance must be requirements-driven, while establishing due diligence under the law must be test-driven.

1. INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA)[1] spurred the adoption of U.S. federal regulations[2] including procedures for protecting the security and privacy of patient health information. In essence, HIPAA regulates all patient record transactions, including paper-based or oral communications.

An electronic health records (EHR) system is a computer-based mechanism to track, store, transmit, and manage patient health and billing information. The iTrust medical records system is an open-source EHR system that was originally developed as a project for a graduate-level software testing and reliability course at North Carolina State University with collaboration from a practicing physician. iTrust has been maintained over several semester-long courses as the project for both undergraduate software engineering and graduate software testing courses. We examined the iTrust Software Requirements Specification (SRS) [7] for compliance with HIPAA, emphasizing the HIPAA's privacy-related regulations[3] as in [3, 4, 6].

We use the term "legal due diligence" to refer to the legal concept of due diligence. Due diligence means "the diligence reasonably expected from, and ordinarily exercised by, a person who seeks to satisfy a legal requirement or to discharge an obligation" [2]. "Requirements compliance" refers to system requirements that are accurately and precisely derived from actual legal texts, whereas "legal compliance" denotes a system that has both requirements compliance as well as a test suite that establishes legal due diligence.

Legal compliance is a major challenge in software engineering [6]. HIPAA regulations were intended to encompass a wide variety of healthcare organizations. As such, the regulations' broad and, at times, ambiguous nature complicates the legal compliance landscape for requirements engineers attempting to implement healthcare software systems. The penalties for non-compliance with HIPAA can be severe. The regulations provide for civil penalties of up to $25,000 per individual per violation and criminal penalties of up to $250,000 and 10 years in prison.

Our case study focused on three primary requirements specification concerns as they relate to legal requirements [6]: (1) prioritizing software requirements to accurately reflect legal priorities, (2) maintaining a traceability link from software requirements to legal texts, and (3) building a glossary to map terminology between software requirements and legal texts.

2. LESSONS LEARNED

Our analysis of the iTrust EHR system revealed the following lessons.

Compliance improves when requirements are closely mapped to governing legal texts.

Specific mappings from requirements to legal statements are necessary to establish due diligence and demonstrate legal compliance [5,6]. The closer the wording between regulatory phrases and the individual requirements in the specification, the easier it is to establish legal compliance and to achieve due diligence. In iTrust, a doctor who is also a patient at a given medical facility would be able to access her own medical records. Through this scenario, among others, we discovered that the iTrust stakeholder roles were disconnected from the HIPAA stakeholder roles to such an extent that tracing between these roles required a many-to-many. By explicitly mapping iTrust stakeholders to the HIPAA stakeholders, it becomes much easier to detect such potential vulnerabilities using traditional testing techniques.

Use cases provide insufficient context to adequately capture and prioritize legal requirements.

Requirements specifications based primarily on a collection of use cases, without including the actual requirements, can introduce contextual problems, lack traceability [1], especially within the context of legal compliance. The iTrust SRS is primarily comprised of a set of use cases that contain preconditions which provide a weak form of prioritization but which lack the rationale necessary to prioritize the software requirements explicitly in the context of the HIPAA. For systems governed by law, legal requirements should be assigned a higher priority than other requirements.

[1] Pub. L. No. 104-191, 110 Stat. 1936 (1996)
[2] 42 C.F.R. §§ 160, 162, 164 (2006)
[3] 42 C.F.R. §§ 164.500–34 (2006)

1090-705x/08 $25.00 © 2008 IEEE
DOI 10.1109/RE.2008.53

Traceability is essential to establish legal due diligence.

Although the iTrust SRS contained a glossary of terminology for its use cases, attempting to map that glossary to the HIPAA terminology was non-trivial: neither the use cases nor the glossary referenced the section within the HIPAA regulations from which a given use case or term originated. Our analysis reveals that iTrust artifacts require more comprehensive traceability to demonstrate legal compliance, especially if legal due diligence is to be established through compliant requirements specification.

Even sophisticated testing techniques cannot detect legal conflicts and ambiguities.

Our case study sought to determine whether a legally compliant system be developed with a test-driven approach. Our analysis revealed that legal compliance must start with requirements. iTrust employs unit testing, which focuses primarily on verification, and scenario testing, which focuses primarily on validation. These techniques can detect internal conflicts and ambiguities in requirements, but have no ability to provide external validation with legal texts. In order to properly detect legal conflicts, ambiguities and vulnerabilities, any testing approach must include explicit validation with the legal requirements in order to establish legal due diligence.

3. DISCUSSION AND FUTURE WORK

Establishing legal compliance encompasses both requirements engineering and software testing. Legal compliance must begin with requirements engineering and end with software testing. No system can establish due diligence with either requirements engineering or testing alone.

If a system is to be developed using test-driven development, the process must be tightly coupled with the applicable legal texts or software requirements that reference legal requirements. iTrust employed test-driven development, but relied on use cases that lacked legal context, prioritization and traceability. A sophisticated testing infrastructure, particularly with a focus on validating legal requirements, can be useful in establishing legal due diligence. Requirements engineers must strive to maintain testable requirements in addition to documenting requirements prioritization, traceability from legal texts to requirements, and an associated glossary of terms.

We limited our analysis to HIPAA regulations, but HIPAA does not preempt other federal or state regulations that may provide stronger privacy or security protections. Consequently, the problems of prioritizing requirements, requirements traceability, and maintaining an accurate glossary of terms become more complex as additional legal texts are considered.

Based on the lessons learned in this case study, we are constructing a new set of requirements for iTrust in order to support our findings here and explore these challenges in more detail. The revised iTrust SRS includes requirements with explicit references to the legal context where appropriate. The previous use cases will be updated to augment the new requirements rather than serving as the primary requirements for the iTrust SRS. Afterwards, we will replicate our case study to further define the core complexities associated with legal requirements.

4. ACKNOWLEDGMENTS

This work was supported by NSF ITR Grant #0325269 and NSF Science of Design Grant #0725144. The authors wish to thank Laurie Williams and Andy Meneely for their participation in interviews throughout our analysis.

5. REFERENCES

[1] A.I. Antón, R.A. Carter, A. Dagnino, J.H. Dempster and D.F. Siege. Deriving Goals from a Use Case Based Requirements Specification, *Requirements Engineering Journal,* Springer-Verlag, Volume 6, pp. 63-73, May 2001.

[2] *Black's Law Dictionary*, 8th ed., Thompson West, 2004.

[3] T.D. Breaux and A.I. Antón. Analyzing goal semantics for rights, permissions, and obligations. *13th IEEE Int'l Requirements Engineering Conf (RE'05),* Paris, France, pp. 177-186, 29 Aug. - 2 Sept. 2005.

[4] T. D. Breaux, M. W. Vail, and A. I. Antón. Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. *14th IEEE Int'l Requirements Engineering Conf (RE'06)*, pages 49–58, Sept. 2006.

[5] P.N. Otto, A.I. Antón, and D. Baumer. The Choicepoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information. *IEEE Security & Privacy*, 5(5), pp. 15-23, Sept./Oct. 2007.

[6] P.N. Otto and A.I. Antón. Addressing Legal Requirements in Requirements Engineering. *15th IEEE Int'l Requirements Engineering Conf*, pp. 5 - 14, 15-19 Oct. 2007.

[7] L. Williams and T. Xie. *iTrust Medical Care Requirements Specification.* Sept. 2007. http://agile.csc.ncsu.edu/iTrust/doc/formalreqs.html