Lab: Compliance Management for HIPPA

Version 1.0

University of Pittsburgh

This is the draft of lab module for SAHI Project

Table of Contents

Lab: Compliance Management for HIPPA

In this lab exercise, you will learn how to extract policy patterns from HIPPA regulations and policies in health care systems, and then formulate a generic policy specification scheme to accommodate those identified patterns.

Part I: HIPAA Overview

The U.S. Health Insurance Portability and Accountability Act (HIPAA) title II was enacted in 1996. HIPAA both explicitly permits certain transfers of personal health information, and prohibits some disclosures: “The privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.” [1]

HIPAA Administrative Simplification, Regulation Text: 45 CFR Parts 160, 162, and 164 regulate the use and disclosure of personal health information. However, as a lab session, we only focus on section 164 of HIPAA, which regulates the security and privacy issues in the health care industry. It covers general pro- visions, security standards for the protection of electronic health information, and privacy of individually identifiable health information.

In this lab, we take section 164.502, 164.506, and 164.508 as an example. You can find the specific regulations online [2-4]. Among them, subpart 164.508 covers uses and disclosures requiring an authorization.

Part II: Modeling HIPAA

Before we model HIPAA, it is necessary to find an application scenario in healthcare domain. As adopted model in our Lab is from paper [1], we also use the medical messaging system as an application scenario in this lab.

Application Scenario

Patients or professionals enter a message into a centralized message system that can “deliver” the message by making it visible to other users. Messages may be simple questions from a patient, or may contain lab test results or other forms of protected medical information. Given information about the message, and other information such as the roles of the sender and receiver in the hospital, the HIPAA compliance module must decide whether delivery of the message complies with HIPAA. To make it simply, we currently focus only on whether to allow a message from a sender to a recipient.

Models

In our application prototype system, our compliance engine is designed to make compliance decisions based on eight message characteristics: *To, From, About, Type, Purpose, In Reply To, Consented By* and *Belief*. The *To* and *From* fields indicate the recipient and sender of the message. The *About* field identifies whose personal health information is contained in the message. The *Type* field defines what kind of information would be passed, such as name or location. The *Purpose* field indicates a reason the message is being sent, such as for medical treatment. The *In* Reply To field was added to describe a disclosure where the message is sent as a response to some earlier message. The *Consented By* field indicates which people have consented to the message disclosure. The *belief* field contains a collection of assertions about the current situation, such as whether this is a medical emergency, or whether disclosure is (in the opinion of the sender) in the best interest of the health of the patient.

Here are some definitions.

Action

For the purpose of determining compliance, a message *action* is represented as an eight-tuple

$a = < u_{src}, u_{dst}, u_{abt}, m_{type}, u_{src}, u_{src}, c, b >$

where

$u_{src}, u_{dst}, u_{abt} \in U$(the set of users or agents)

$m_{typ} \in T$ (the set of types of messages)

$m_{pur} \in P$ (the set of purposes)

$a_{reply} \in A$(the set of actions)

$c =< u_{by}, ct_{typ} > \in C$ (the tuple of consents) where

$u_{by} \in U$ (the set of users)

$ct_{typ} \in CT$ (the set of consent types)

$b =< u_{by}, u_{abt}, bf > \in B$ (the tuple of beliefs) with

$u_{by}, u_{abt} \in U$ (the set of users)

$bf \in T$ (the set of beliefs)

HIPAA Policy

A HIPAA policy is a function from actions to Booleans (true or false), indicating permission or prohibition.

$U \times U \times U \times T \times P \times A \times C \times B \rightarrow \{\text{T,F}\}$

Categories

A category is a set of field values defining the conditions when a legal clause is applicable to a particular action. For example, one common category of actions is those with type indicating protected health information and purpose indicating medical treatment.

Subcategories

Naturally, some field values may indicate that the action belongs to a subcategory of another category of actions. For example, psychotherapy note is a subtype of health records, which implies that policy about health records could also affect decisions about psychotherapy note, but not vise versa. More generally, the possible values associated with any field may be partially ordered.

Roles

While it is possible to express policy about specific individuals, HIPAA policies are written using roles. For example, an individual could be a nurse or a doctor. When an action is considered, our system receives the names of the sender and recipient, for example, and then uses information about the hospital to determine the respective role(s). For patients, similar processing (formalized in Prolog) is used to determine whether the patient is an adult or a minor.

Formalization of HIPAA

Here we use 164.508.a.2 f HIPAA as an example to illustrate the structure of a clause of HIPAA.

§164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: Authorizations for uses and disclosures* -- (2) *Authorization required: Psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:(A) Use by the originator of the psychotherapy notes for treatment;(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by §164.502(a)(2)(ii) or permitted by §164.512(a); §164.512(d) with respect to the oversight of the originator of the psychotherapy notes; §164.512(g)(1); or §164.512(j)(1)(i).

Simply, 164.508.a.2 states, among other things, that a covered entity must obtain an authorization for any use or disclosure of psychotherapy note, except if it is to be used by the originator of the psychotherapy note for treatment.

Requirement

An action that falls into the category of a legal clause is allowed only if the requirement in the clause is satisfied. For example, 164.508.a.2 states that the specified action is allowed only if an authorization is obtained.

Exception

An exception in a legal clause qualifies its category. For example, 164.508.a.2 states that if the purpose of the action is for use by the originator of the psychotherapy note for treatment, then the requirement does not apply.

Clause vs. Rule

For ease of exposition, we call a labeled paragraph in the HIPAA law a clause, and its translation into logic rules. To illustrate our terminology, a clause with *category* given by predicate *a*, *requirement* predicate *c* and *exceptions e* can be expressed as the following rules:

$$permitted\_by_R \Leftarrow (a \wedge \neg e) \wedge c$$

$$forbidded\_by_R \Leftarrow (a \wedge \neg e) \wedge \neg c$$

$$R\_not\_applicable_R \Leftarrow \neg a \wedge e$$

Combination

A central concept in our approach is the way that a policy composed of several legal clauses is expressed by a combination of the associated *permitted_by* and *forbidden_by* rules. Given rules $R_1 \ldots R_m$, any action is consistent with the policy of these rules if it is permitted by some of the rules and not *forbidden_by* any of them.

$$compliant_{R1 \ldots Rm} \Leftarrow \left(permitted_{by_{R1}} \vee \ldots \vee permitted_{by_{Rm}}\right) \wedge$$

$$\neg(forbidded\_by_{R1} \vee \ldots \vee forbidded\_by_{Rm})$$

Exercise:

Read the following clauses of HIPAA and try to encode them.

164.502.b Standard: Minimum necessary

164.502.b.1 Minimum necessary applies.

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

164.502.b.2 Minimum necessary does not apply.

This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

Q: Based on the previous model and definitions, what is the *category* for this clause? (For example, *from, to, type, belief, exception, et al.*)

Q: Try to figure out the logic translation of this clause.

$$permitted_{by_{R_{502b}}}(A), forbidden_{by_{R_{502b}}}(A)$$

Read another segments of HIPAA and answer the question.

164.502 Uses and disclosure of protected health information

164.502.a Standard: A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

164.502.a.1 Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with 164.506;

Q: What is the *category* for this clause?

Q: Try to figure out the logic translation of this clause.

Q: Suppose that the total HIPAA is the above two clauses, give the compliant HIPAA policy based on your logic translation.

Now we put some attributes and relations in our application scenario.
We can define attributes and relations.
Consider a relation called *inRole* that identify a particular individual and their role.
Suppose that C, a nurse and D, a doctor are working for the UPMC and R_{506} is satisfied.

inRole(C, nurse)
inRole(D, doctor)
inRole(doctor, covered entity)
inRole(nurse, covered entity)
inRole(UPMC, covered entity)
employeeOf(UPMC, D)
employeeOf(UPMC, C)

Q: Based on this information and your logic translation rule of HIPAA, can an *action*, like the following, be passed by compliance system?
(from : C, to : D, type : health records, for : treatment)

Q: How about this *action*?
(from : C, to : xyz, type : health records, for : treatment)

Open Question:

Q: Consider the above scenario, we suppose that R_{506} is satisfied. Please try to remove that assumption and combine clauses in 506 of HIPAA and then construct your logic translations and apply to the scenario.

Q: Consider the cross reference situation, that is, a requirement of a clause involves a reference to other clause of the law. Suppose that Rule A require Rule B, Ruble B depend on Rule C, but Rule C rely on Rule A. Can you provide a simple solution for that your logic translations could make a final decision? Give a brief explanation.

References

1 Lam, P. E., Mitchell, J. C., & Sundaram, S. (2009). A Formalization of HIPAA for a Medical Messaging System. *Lecture Notes in Computer Science*, *5695*, 73.

2 http://www.ecfr.gov/cgi-bin/text-idx?SID=9584f641683cc2aa82b2ad2b90aab46b&mc=true&node=se45.1.164_1502&rgn=div8

3 http://www.ecfr.gov/cgi-bin/text-idx?SID=9584f641683cc2aa82b2ad2b90aab46b&mc=true&node=se45.1.164_1506&rgn=div8

4 http://www.ecfr.gov/cgi-bin/text-idx?SID=9584f641683cc2aa82b2ad2b90aab46b&mc=true&node=se45.1.164_1508&rgn=div8