Strategic Healthcare IT Advanced Research Projects on Security
SHARPS

Modeling State Privacy Laws: *Analyzing Alabama and Alaska*

TRUST | CURIS | Final Research Report

Ashley Tolbert
TRUST/CURIS Undergraduate Research Program
Auburn University
Auburn, AL, U.S.A.
art0008@auburn.edu

Ellick Chan, Peifung E. Lam, John C. Mitchell
Department of Computer Science
Stanford University, SHARPS
Stanford, CA, U.S.A
emchan@stanford.edu, ericlam@stanford.edu,
mitchell@cs.stanford.edu

***Abstract*—The complexity of regulations in healthcare, financial services, and other industries makes it difficult for enterprises to design and deploy effective compliance systems. We believe that in some applications, it may be practical to support compliance by using formalized portions of applicable laws to regulate business processes that use information systems. In order to explore this possibility, we use a stratified fragment of Prolog with limited use of negation to formalize a portion of the US Health Insurance Portability and Accountability Act (HIPAA). As part of our study, we also explore the deployment of our formalization in a prototype hospital Web portal messaging system [1].**

I. Introduction

In regulated sectors such as healthcare, finance, and accounting, laws such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, and related European laws have been enacted over the past decade to establish new or enhanced standards. The length of these laws, the opacity of the legal language, and the complexity of these acts make it very difficult for practitioners to determine whether they are in compliance. This complexity becomes even more significant if computer programmers and information technology professionals wish to build and configure automated systems to help business professionals comply with applicable laws [1].

In our research project conducted in the Department of Computer Science at Stanford University, we will analyze the privacy issues faced by the healthcare industry and how we attempt to help address theses challenges using logic and encryption.

II. Project Goals and Objectives

The project goal is to construct a compliance Prolog module that can decide, as messages are composed or entered into the system, whether a message complies with HIPAA. We also hope to produce a formalization that could be verifiable by lawyers, medical and computer professionals alike.

In the application that we are hoping to produce, 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.

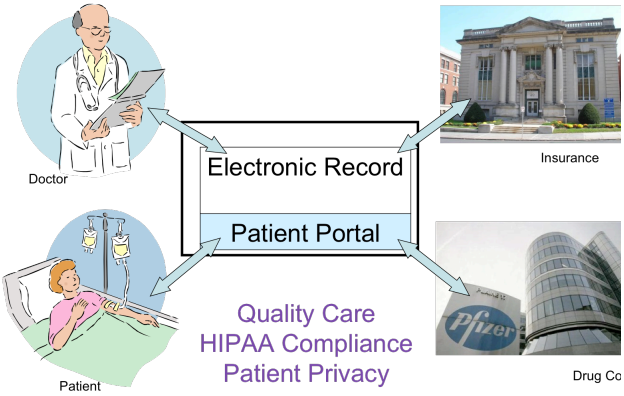

Fig. 1. The Healthcare Privacy Problem. *The goal is to respect privacy expectations in the transfer and use of personal information within and across organizational boundaries.*

Fig. 2. Privacy in Organizations Processes

While portions of HIPAA regulate how data may be used after it is disclosed, or specify notifications that must be given after

the disclosure, we currently focus only on whether to allow a message from a sender to a recipient [1].

Record Type	Patient	Family	Healthcare Providers	Gov.
Mental Health	YES w/ healthcare provider consent	YES if primary caretaker, cohabitant or parent of minor	YES w/o consent of patient	YES w/o consent if investigating fatal crime
Substance Abuse	YES	YES if primary caretaker or parent of minor	YES w/o consent if believed to be "necessary to treatment"	YES w/ patient consent
STD	YES	YES if primary caretaker or parent of minor	YES w/o consent of patient	YES w/ patient consent
Genetic Information	YES	YES w/ patient consent	YES w/o consent if believed to be "necessary to treatment"	YES w/o consent if investigating crime or paternity

Fig. 3. State Laws Template. *This is the template used to collect data of state laws*.

Hopefully, this tool with help to highlight contradictions and discrepancies between state laws and HIPAA laws concerning the permissions to record requesters and the access of patient health records.

III. Methods

A. Data Collection

The method that was used for data collection included a template listing the permissions for access to patient health records falling under the four categories of conditions: mental health, substance abuse, STD, and genetic information. Then,

the permission for access to the conditional records is separated by the four types of requesters falling under the categories of the patient themselves, a healthcare provider, the government, or an insurance company.

States were analyzed and researched for the permission of access to records for the conditions in these states and the results were compiled in a YES/NO system that also lists the exceptions.

B. Formulation of Prolog

The method that was used for the formulation of the Prolog code included converting the data collected in the state laws templates into a message in Prolog. This strategy includes a clause that implies that when a covered entity is sending health records for the purposes of treatment then it should also comply with the clause. Here the category is from: a covered entity and type: health records and purpose: treatment. The requirement is to comply with the clause. Thus the logic translation of the two clauses would look like that depicted in Figure 4.

IV. Research Issues Found: Alabama and Alaska

The results for the research were very substantial. Although the information gathered is that from two states, Alabama and Alaska, the information is quite significant considering the types of states that the two are – Alabama being a small, southern state and Alaska being a distant, secluded northern state.

A. Alabama

Alabama states laws concerning the access of patient health records are, compared to other states, lacking in clauses

Rules:-

$$permitted\_by_{R_{502b}}(A) \Leftarrow (A_{from} = covered\ entity) \wedge (A_{type} = health\ records) \wedge (A_{to} = covered\ entity) \wedge \neg(A_{purpose} = treatment) \wedge (A_{belief} = minimal)$$

$$forbidden\_by_{R_{502b}}(A) \Leftarrow (A_{from} = covered\ entity) \wedge (A_{type} = health\ records) \wedge (A_{to} = covered\ entity) \wedge \neg(A_{purpose} = treatment) \wedge \neg(A_{belief} = minimal)$$

$$permitted\_by_{R_{502aii}}(A) \Leftarrow (A_{from} = covered\ entity) \wedge (A_{type} = health\ records) \wedge (A_{purpose} = treatment) \wedge permitted\_by_{R_{506}}(A)$$

$$forbidden\_by_{R_{502aii}}(A) \Leftarrow (A_{from} = covered\ entity) \wedge (A_{type} = health\ records) \wedge (A_{purpose} = treatment) \wedge forbidden\_by_{R_{506}}(A)$$

Policy:-

$$compliant\_with_{HIPAA} \Leftarrow permitted\_by_{R_{502b}} \vee permitted\_by_{R_{502aii}} \wedge \neg(forbidden\_by_{R_{502b}} \vee forbidden\_by_{R_{502aii}})$$

Attributes:-

We can define attributes and relations. Consider a relation called *inRole* that identify a particular individual and their role. It is simple to consider an example from the sitcom *Scrubs* where *dr_cox*, a doctor and *carla*, a nurse work for the *Sacred Heart Hospital*.

$$inRole(carla, nurse)$$
$$inRole(dr\_cox, doctor)$$
$$inRole(doctor, covered\ entity)$$
$$inRole(nurse, covered\ entity)$$
$$inRole(sacredHeart, covered\ entity)$$
$$employeeOf(sacredHeart, dr\_cox)$$
$$employeeOf(sacredHeart, carla)$$

We can also have a transitive closure of these rules which would imply that *carla* and *dr_cox* are *covered entity*.

Given this policy and the list of attributes, assuming *dr_cox* and *carla* work for the same hospital and R_{506} is satisfied, an action that would be allowed with this particular rule system is:

$$(from : carla, to : dr\_cox, type : health\ records, for : treatment)$$

Fig. 4. Prolog Code Message Formulation. *This is an image illustrating the rules of how the Prolog code that is formulated from the state laws.*

for significant rules. For example, Alabama does not have a general, comprehensive statute granting patients the right to see and copy their own medical records. Neither does the state have a general statute restricting the disclosure of confidential medical information. The Alabama Code does, however, restrict disclosures by health maintenance organizations.

Additionally, Alabama has some statutes that govern a patient's access to and the disclosure of information related to specific medical conditions, such as mental health and sexually transmitted diseases [2].

We examined the laws concerning patient record access across for Alabama and these are the most salient issues found:

- **STD Records: Patients/Families and Healthcare Providers [Ala. Code § 22-11A-38.]**
  1. Under Alabama laws, yes, patients have rights to access and release information included in disease and medical records with the approval from a professional staff member.
  2. However, staff members are required to send mandatory reports to higher office of every case of disease detected to identify and prevent the spread of disease.
  3. However, there are a number of exceptions that apply. Physicians may disclose if there is a foreseeable risk of transmission of the disease.

- **Genetic Information Records: Any Requester Ala. Code § 27-21A-25.]**
  1. Alabama does not have a genetic comprehensive statute granting patients the right to see and copy their own medical records. Neither does the state have a general statute restricting the disclosure of confidential medical information

- **Mental Health, STD, or Substance Abuse Records: Healthcare Providers release to Government, Insurance Providers, etc. [Ala. Code § 22-56-4(b)(7).]**
  2. Under Alabama law, when released by the patient to health care providers, health care providers then have the permission to release records to any related third party outsider in any case of emergency or when there is a foreseeable risk of emergency.

Conclusively, Alabama lacks many important laws that can alter the outcome of many legal situations. The relevant health care provider mainly dominates overall, patient record access control.

B. Alaska

Alaska state laws concerning the access of patient health records are rather differential from those of other states. We chose to examine the state of Alaska because of its significant distance from other states and because it is a Republican state. Upon these observations, we believed that Alaska would prove to be quite a distinctive state in comparison to other states' patient record access laws. These are the most salient issues found:

- **Mental Health Records: Government Access [Alaska Stat. § 47.30.845(8).] [Alaska Stat. § 47.30.845(5).] [Alaska Stat. § 47.30.845(6).] [Alaska Stat. § 47.30.845(7).]**
  1. The Department of Corrections can access records when a prisoner confined to the state prison is transferred to a state hospital.
  2. A law enforcement or governmental agency can access records when necessary to secure the return of a patient who is on unauthorized absence from a facility where the patient was undergoing evaluation or treatment.
  3. A law enforcement agency can access records when there is a substantial concern over imminent danger to the community by a presumed mentally ill person.
  4. The Department of Health and Social Services can access records where services are paid through assistance provided under Alaska state.

- **Substance Abuse Records: Healthcare Provider Access [Alaska Admin. Code tit. 7, § 27.005 (2001).]**
  1. Substance abuse records can be obtained by health care providers without the consent of the patient in a need-based situation.
- **Genetic Information Records: Government and Insurance Providers Access [Alaska Stat. § 40.25.120.]**
  1. No, medical and related public health records are not open to public inspection under the state Freedom of Information Act, but can be accessed by patient's consent.

Conclusively, the health care providers and the government dominate Alaska patient health record access, which in comparison to other states, is unusual because of most states granting overall permission of health records to the patients.

V. Results/Outcome

A. Results

```
permitted_by_AL_22_56_4b7(A):-
  is_msg_type(A, mental_health),
  msg_to(A, X),
  msg_about(A, X),
  is_msg_consented(A,Y),
  in_role(Y, healthcare_provider).

is_msg_type(a(_,_,_,Y,_,_,_,_), Y).
msg_to(a(X,_,_,_,_,_,_,_), X).
msg_about(a(_,_,X,_,_,_,_,_), X).
is_msg_consented(a(_,_,_,_,_,_,(X,consented),_),X).
in_role(dr_cox,healthcare_provider).
```

Fig. 5. Alabama Law Prolog Code. This image shows a snippet of the Alabama laws formulated into Prolog code using the messaging system.

Conclusively, we were able to construct the laws detailing the access permissions of Alabama and Alaska into Prolog code. Shown in Figure 5 is a snippet of the code derived for the Alabama laws.

B. Outcome

Additionally, we were able to chart the gaps of difference in permission control dominance for both Alabama and Alaska. Shown in Figure 6 is a pie chart illustrating the dominance for the states for patient control, healthcare provider control, government control, and insurance providers control.

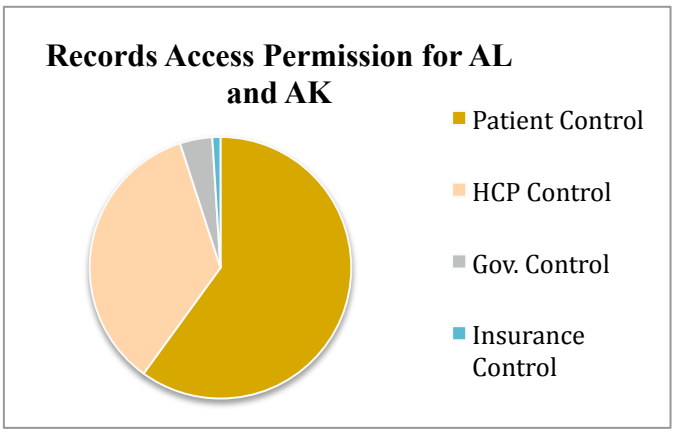

Fig. 6. Pie Chart of Access Control Dominance. This image shows the permission dominance for Alabama and Alaska.

VI. Conclusion/Future Work

In conclusion, the research was a success, although only a few states were taken into consideration. However, the research will continue with all 50 states. Once all 50 states are done, the states can be categorized and grouped into clusters of states with similar laws. Once this has been done, the messaging system can continue with much more information to be considered.

A number of possible future directions seem promising. While we have not formalized all parts of HIPAA, it is possible to continue the effort to other portions of the law, if desired. We also look forward to collaborating with others, in hopes that there could be an open-source HIPPA formalization process. By sharing a formal presentation of HIPAA among many researchers and healthcare organizations, it may be possible to develop confidence in the formal presentation and use it widely across many enterprises [1].

Acknowledgment

A distinguished thank you to the TRUST (Team for Research in Ubiquitous Secure Technology) program staff, CURIS (Computer Science Undergraduate Research Internship) program staff, and the National Science Foundation for the support throughout this research experience. Also, A special thank you to Dr. John C. Mitchell, Peifung E. Lam, and Ellick Chan for serving as mentors for the project and helping with the research.

References

[1] Lam, Peifung E., Mitchell, John C., and Sundaram, Sharada. "A Formalization of HIPAA for a Medical Messaging System", Stanford University, Stanford, CA, 2009. (August 10, 2012). Available at SSRN: www-cs-students.stanford.edu/~pflam/research/HIPAA_formalization.TB 2009.pdf

[2] Dr. Janlori Goldman. The State of Health Privacy Volume 1: A Survey of State Health Privacy Statues. Institute for Healthcare Research and Policy Georgetown University Journal, 9(1):3–17, 2010.

[3] Dr. Janlori Goldman. The State of Health Privacy Volume 2: A Survey of State Health Privacy Statues. Institute for Healthcare Research and Policy Georgetown University Journal, 6(1):8–12, 2010.

[4] Chan, E., Lam, P., Mitchell, J., Rajan, S., Siddiqui, S., and Tolbert, A. "Modeling State Privacy Laws", Stanford University, Stanford, CA, 2012 unpublished.

[5] Dr. Joy Pritts and Marisa Guevara. Your Medical Records Rights in Alaska. [August 4, 2012.] http://www.hpi.georgetown.edu/privacy/stateguides/ak/ak

Appendix A: State Laws Template

		Patients (Adult)
	Mental health	Yes, patients have a st right to access to all information included in health and medical rec with the approval from professional staff mem
	Substance Abuse	Yes, patients can acce substance abuse recor without Adjust table professional.
	STD	Yes, patients have righ access to all informatio included in disease and medical records with th approval from a profess staff member Staff members are requ send mandatory reports higher office of every ca disease detected.

APPENDIX B: PROLOG FORMULATION

```
% Prolog Code: State Laws Project
% Alabama State Laws
% Regarding access to state laws, specifically records of the
% specific types mental health, cancer, STD, and genetic information.

Rules:

permitted_by_AL_22_56_4b7(A):-
  is_msg_type(A, mental_health),
  msg_to(A, X),
  msg_about(A, X),
  is_msg_consented(A,Y),
  in_role(Y, healthcare_provider).

is_msg_type(a(_,_,_,Y,_,_,_,_), Y).
msg_to(a(X,_,_,_,_,_,_,_), X).
msg_about(a(_,_,X,_,_,_,_,_), X).
is_msg_consented(a(_,_,_,_,_,_,(X,consented),_),X).
in_role(dr_cox,healthcare_provider).

Query:

permitted_by_AL_22_56_4b7(a(alice, dr_cox, alice, mental_health, patient_request, prev_me
                (dr_cox, consented) ))
```