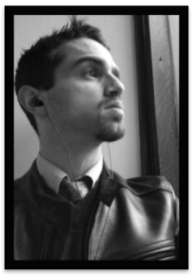
Assessing Regulatory Change through Legal Requirements Coverage Modeling

David G. Gordon and Travis D. Breaux (CMU, USA)



Name: David Gordon

Email: dggordon@cmu.edu

Affiliation: Department of Engineering and Public Policy at Carnegie Mellon University

David Gordon is a 4th year PhD student at Carnegie Mellon University in the department of Engineering and Public Policy. Working with his advisor, Travis Breaux, his research focuses on addressing the difficulties of multi-jurisdictional legal compliance that affect system design. In this work, he proposes a method for legal requirements coverage modeling, and shows how coverage can change as organizations encounter new regulations, move their services abroad, or introduce new product features.

Carnegie Mellon

Problem

- Increasing regulation for information privacy and security
  - USA, EU, India, South Korea
- Compliance is nontrivial and expensive
  - Healthcare Data Breach: est. $7b in 2013 *(Ponemon Institute, 2013)*
- Coverage determination is complicated
- Complexity compounded by changing laws and systems

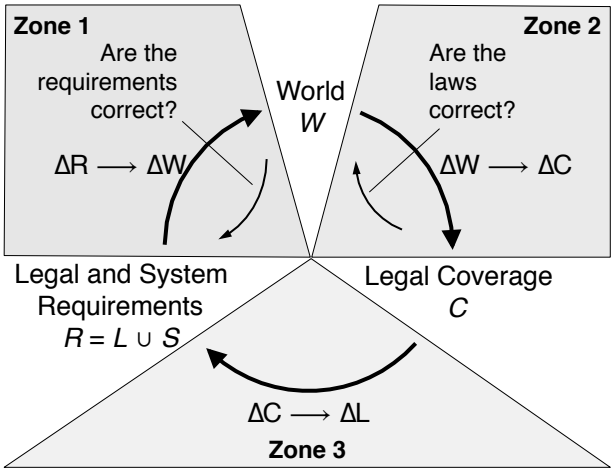
Coverage Modeling

- Process structures regulation as set of requirements, conditions
- Conditions satisfied for requirement, implicated on organization
- Conditions reused, affect one another
- Analyst supplies model with information to find relevant requirements to organization

Research Questions

- **RQ_1**: How do we determine the minimum set of questions for a given law?
- **RQ_2**: How does coverage change when an organization...
  - $RQ_{2\text{-}1}$: introduces a new product feature
  - $RQ_{2\text{-}2}$: outsources a component of its services abroad
  - $RQ_{2\text{-}3}$: faces a new or updated law

Legal Requirements Lifecycle



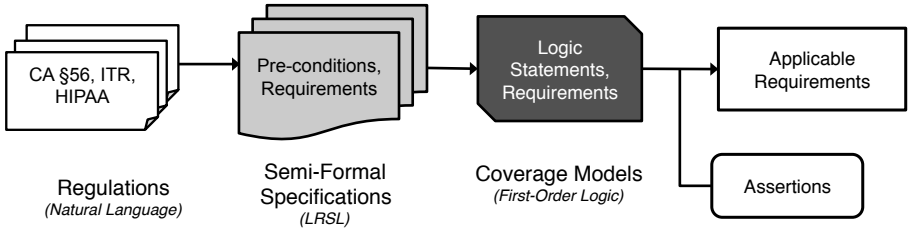
Case Study Design

1. Develop hypothetical organization and real-world scenarios
2. Generate regulatory coverage models
   1. Translate regulation into LRSL
   2. Generate model logic using denotational semantics
3. Determine coverage change in scenarios by traversing models

Agenda

- Introduction
- Coverage Modeling
- Summary Findings
- Scenario Outcomes
- Related Work
- Future Work and Summary

Coverage Model Definition



- Structured representation of natural language regulation into pre-conditions
- Expressed in first-order logic
- Corresponding legal requirements entailed by satisfying propositions using assertions

CM-1: Translate into LRSL

5. (1) Body Corporate or person on its behalf... collects sensitive personal data or information...

(3) ***When*** *collecting information directly from the person concerned, body corporate or any person on its behalf…* ***shall ensure*** *that the person concerned is having knowledge of... the purpose for which the information is being collected*

6. (1) Disclosure of sensitive personal data or information by body corporate to any third party ***shall require*** *prior permission from the provider of such information…* ***unless*** *the disclosure is necessary for compliance of a legal obligation.*

Excerpts from India's ITR §§5 and 6


```
SECTION ITR.5 //Collection of information
PAR (1)
body corporate
   | any person on behalf of the body corporate
   : collects sensitive personal data
PAR (3)
   : collecting information directly from the person
     concerned
   REFINES (1) #1
   : shall ensure the person concerned is having the
     knowledge of the purpose [of collection]
   REFINES (3) #1
SECTION ITR.6 //Disclosure of information
PAR (1)
body corporate
   : may disclose sensitive personal data... to any
     third party
   FOLLOWS ITR.5(1) #1
   : shall require permission from the provider of
     such information...
   PRECEDES ITR.6(1) #1
   : it is necessary for compliance of a legal
     obligation
   PRECEDES (1) #4
   : must make the disclosure
   EXCEPT-TO ITR.6(1) #2
```

(Breaux and Gordon, 2013)

Document Structure
Preserves document references for traceability

Stakeholders
Actors to whom conditions and requirements apply

```
SECTION ITR.5 //Collection of information
PAR (1)
body corporate
   | any person on behalf of the body corporate
   : collects sensitive personal data
PAR (3)
   : collecting information directly from the person
     concerned
   REFINES (1) #1
   : shall ensure the person concerned is having the
     knowledge of the purpose [of collection]
   REFINES (3) #1
SECTION ITR.6 //Disclosure of information
PAR (1)
body corporate
   : may disclose sensitive personal data... to any
     third party
   FOLLOWS ITR.5(1) #1
   : shall require permission from the provider of
     such information...
   PRECEDES ITR.6(1) #1
   : it is necessary for compliance of a legal
     obligation
   PRECEDES (1) #4
   : must make the disclosure
   EXCEPT-TO ITR.6(1) #2
```

(Breaux and Gordon, 2013)

Document Structure
Preserves document references for traceability

Stakeholders
Actors to whom conditions and requirements apply

Non-Modals
Criteria precipitating occurrence of an event

Requirements
Obligation, permission, prohibition placed on a stakeholder

```
SECTION ITR.5 //Collection of information
PAR (1)
body corporate
   | any person on behalf of the body corporate
   : collects sensitive personal data
PAR (3)
   : collecting information directly from the person
     concerned
   REFINES (1) #1
   : shall ensure the person concerned is having the
     knowledge of the purpose [of collection]
   REFINES (3) #1
SECTION ITR.6 //Disclosure of information
PAR (1)
body corporate
   : may disclose sensitive personal data... to any
     third party
   FOLLOWS ITR.5(1) #1
   : shall require permission from the provider of
     such information...
   PRECEDES ITR.6(1) #1
   : it is necessary for compliance of a legal
     obligation
   PRECEDES (1) #4
   : must make the disclosure
   EXCEPT-TO ITR.6(1) #2
```

(Breaux and Gordon, 2013)

Document Structure
Preserves document references for traceability

Stakeholders
Actors to whom conditions and requirements apply

Non-Modals
Criteria precipitating occurrence of an event

Requirements
Obligation, permission, prohibition placed on a stakeholder

Relation
Reflects relationship between requirements and conditions

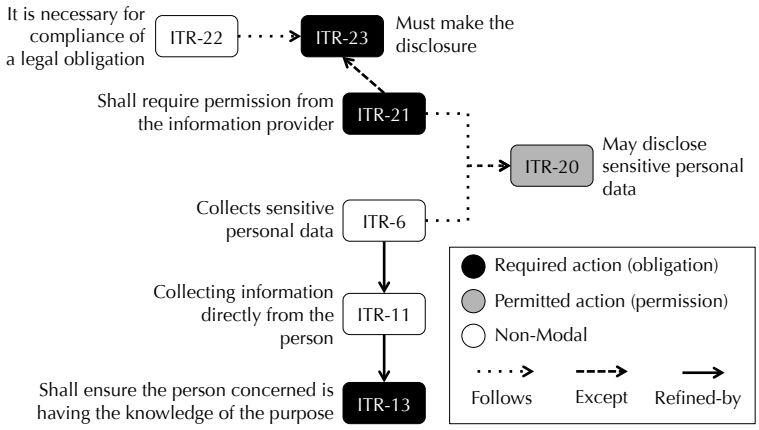
```
SECTION ITR.5 //Collection of information
PAR (1)
body corporate
   | any person on behalf of the body corporate
   : collects sensitive personal data
PAR (3)
   : collecting information directly from the person
     concerned
   REFINES (1) #1
   : shall ensure the person concerned is having the
     knowledge of the purpose [of collection]
   REFINES (3) #1
SECTION ITR.6 //Disclosure of information
PAR (1)
body corporate
   : may disclose sensitive personal data... to any
     third party
   FOLLOWS ITR.5(1) #1
   : shall require permission from the provider of
     such information...
   PRECEDES ITR.6(1) #1
   : it is necessary for compliance of a legal
     obligation
   PRECEDES (1) #4
   : must make the disclosure
   EXCEPT-TO ITR.6(1) #2
```

(Breaux and Gordon, 2013)

Definitions
Terms-of-art that elaborate on certain concepts, notably stakeholders

```
SECTION ITR.2 //Definitions
PAR (c)
body corporate    //ITR-A1
   < company      //ITR-A1_1
      | firm      //ITR-A1_2
      | sole proprietorship          //ITR-A1_3
      | association of individuals   //ITR-A1_4
         & engaged in commercial or
           professional activities  //ITR-A1_5
```

CM-1: LRSL Graphs



CM-2: LRSL to Logic Expressions

Term	Definition
G	LRSL-Generated Graph
V(G) *- REQ(G)* *- NON(G)*	Set of Vertices - Subset of legal requirements - Subset of non-modal actions
E(G) *- REFINED-BY(G)* *- EXCEPT(G)* *- FOLLOWS(G)*	Set of Edges - Subset of REFINED-BY edges - Subset of EXCEPT edges - Subset of FOLLOWS edges

$1: expr[\![v \in REQ(G)]\!] = lhs[\![v]\!] + " \rightarrow " + rhs[\![v]\!]$
$2: lhs[\![v]\!] = actor[\![v]\!] + edges[\![v]\!]$
$3: edges[\![(v,w) \in FOLLOWS(G) \cup REFINES(G)]\!] = "\wedge" + rhs[\![w]\!]$
$4: edges[\![(v,w) \in EXCEPT(G)]\!] = "\wedge \neg(" + rhs[\![w]\!] + ")"$
$5: rhs[\![v \in NON(G)]\!] = actor[\![v]\!] + " \wedge performs\_v" + edges[\![v]\!]$
$6: rhs[\![v \in REQ(G)]\!] = "covered\_v"$

CM-3: Traversing the Model

(ITR-A1 ∨ ITR-A2) ∧ performs_ITR-11 ∧ performs_ITR-6 → covered_ITR-13

Prop.	Assertion	Evidence
ITR-A1$_1$ (company)	W1: organization is incorporated under Sec. 242 of General Corporation Law of Delaware	Delaware Non-Stock Certification of Incorporation Form
performs_ITR-6	W2: organization collects medical information from patient	Incoming Patient Form #8675309
performs_ITR-11	W3: organization collects personal information directly from patient	Incoming Patient Form #8675309

Agenda

- Introduction
- Coverage Modeling
- Summary Findings
- Scenario Outcomes
- Related Work
- Future Work and Summary

Data Set Selection

Largest Healthcare Industry

California

Confidentiality of Medical Records Act
(CC. §56 et seq.)
1981-2011

Recently issued New Regulation

India

Information Technology Rules
(ITR)
2011

Minimum Floor, Recently Updated

United States

Health Insurance Portability and Accountability Act
(HIPAA)
2003 - 2010

Requirement/Relational Counts

	Timing		# Requirements			# Relations		
	Total (hrs)	mins/req	NM	O	P	R	E	F
CA	2.5	2.2	4	18	2	18	5	3
ITR	4.0	1.6	6	15	2	14	2	10
HIPAA	14	4.9	10	38	3	29	5	9

NM: *non-modal*, O: *obligations*, P: *permissions*
R: `REFINES`, E: `EXCEPT`, F: `FOLLOWS`

RQ_1: Minimum Questions

- Dependent on number of stakeholders and non-modal actions
- Influenced by ground truth, and analyst's rigor

	# Questions (L)	# Questions (U)
CA	7	22
ITR	2	12
HIPAA	2	53

L (lowerbound): *organization is not covered; fewest assertions made by analyst*
U (upperbound): *organization is covered, most assertions made by analyst*

Hypothetical Organization

- Initial Requirements from *Certification Commission for Healthcare Information Technology* (CCHIT) Ambulatory EHR Criteria:

AM 01.01: ...create a single patient record for each patient.

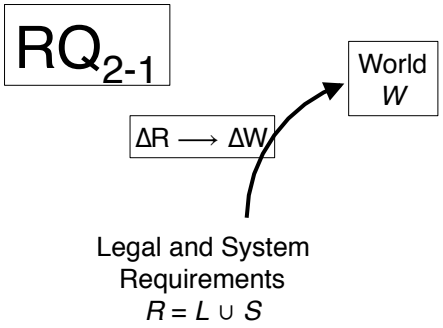
AM 02.01: ...provide the ability to include demographic information in reports.

FN 04.02: ...provide the ability to capture, maintain and display, as discrete data elements, all problems/diagnoses associated with a patient.

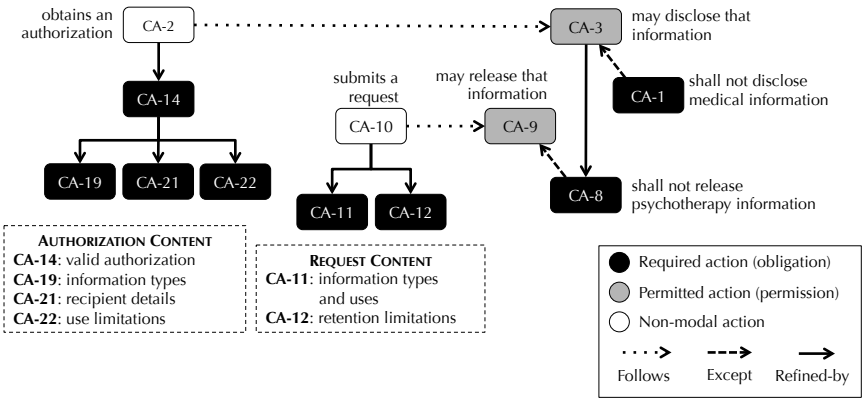
AM 26.01: ...have the ability to provide electronic communication between prescribers and pharmacies or other intended recipients of the medication order.

AM 39.01: ...provide the ability to export (extract) pre-defined set(s) of data out of the system.

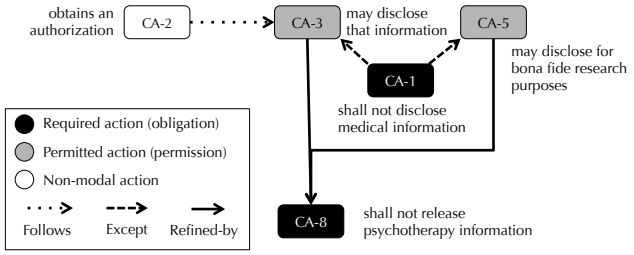
$RQ_{2\text{-}1}$: New Product Feature



$RQ_{2\text{-}1}$: New Product Feature

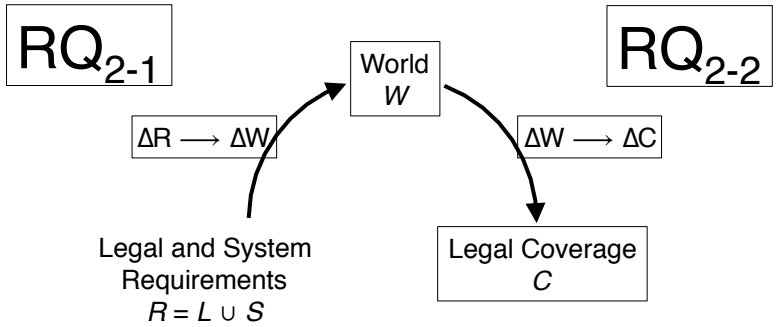


$RQ_{2\text{-}1}$: New Product Feature

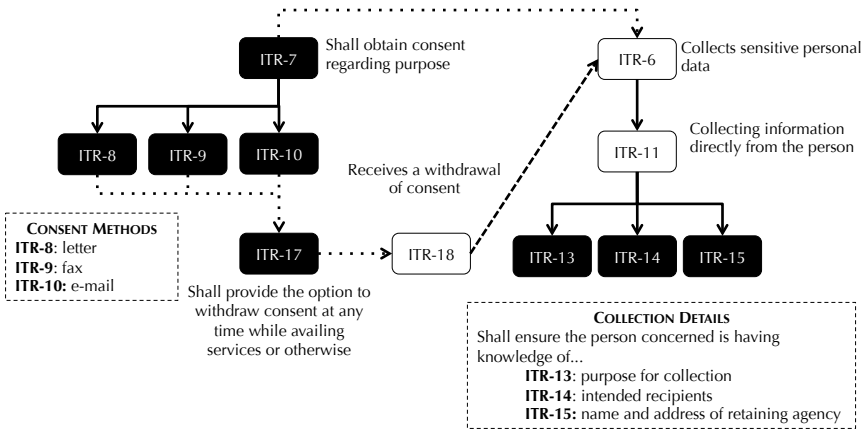


Δ	Description	
ΔS	Requirements implementing research disclosure mechanisms	
ΔW	Assertions regarding disclosure to third parties for research purposes, evidenced by contracts describing research purposes, constraints on use, etc.	
ΔL	*health care provider* **CA-5**: permission to disclose for research	*contractor* **CA-14 – CA-24**: obligation to obtain authorization for disclosure and refinements detailing that procedure

$RQ_{2\text{-}2}$: Outsources Abroad



$RQ_{2\text{-}2}$: Moving Abroad

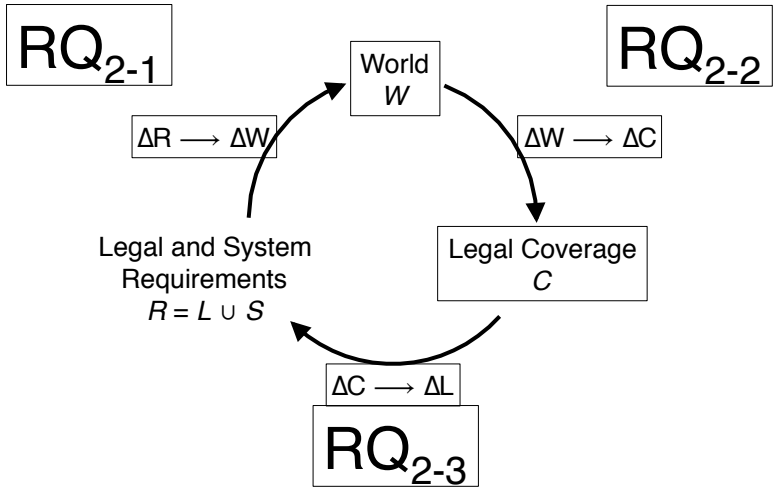


$RQ_{2\text{-}2}$: Moving Abroad

Δ	Description
ΔS	Identification of requirements for medical data transcription service
ΔW	Assertions to perform medical information processing in India
ΔL	*body corporate* **ITR-7 – ITR-10**: obtaining data subject consent **ITR-13 – ITR-15**: data subject awareness of purpose and recipient of information **ITR-17**: providing option to withdraw consent

- Additional burden of requirements from India
- Significant expansion of consent requirements
- Produces high water mark effect *(Gordon and Breaux, 2012)*

RQ_{2-3}: Regulatory Change



RQ_{2-3}: Regulatory Change

- HIPAA updated by Health Information Technology for Economic and Clinical Health (HITECH) Act
- New conditions (ΔC) given current assertions (W), implicates new requirements (ΔL)
- Includes many new provisions, notably data breach notification requirements
- New coverage mechanism in HP-51: business associate agreements

$RQ_{2\text{-}3}$: Regulatory Change

- Business Associate Agreements (BAA) – contracts between covered entities and business associate, spreads coverage of Security and Privacy Rule

Risk Analysis (*Required*). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Automatic Logoff (*Addressable*). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Audit Controls (*Addressable*). Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Mechanism to authenticate electronic protected health information (*Addressable*). Implement a mechanism to authenticate electronic protected health information and to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Agenda

- Introduction
- Coverage Modeling
- Summary Findings
- Scenario Outcomes
- Related Work
- Future Work and Summary

Related Work

- Legal formalization and laws as logic
  (Biagoli et al., 1987; Sergot et al., 1986)
- Adoption, interpretation of law in requirements engineering *(Breaux et al., 2006 and 2008)*
- Regulatory change and external referencing
  (Maxwell et al., 2009, 2012)
- Regulations as norms using Nómos 2
  (Siena et al., 2011)

Summary and Future Work

- Legal coverage is complex, nuanced
- Preliminary framework for identification of relevant legal requirements and coverage changes
- Small step towards semi-automated reasoning of legal coverage for IT systems
- Scalability and multi-jurisdictional issues remain a concern

Acknowledgements

- Ashwini Rao and Hanan Hibshi
- Hewlett-Packard (HP) Labs Innovation Research Program Award #CW267287 and the HP Cloud and Security Laboratory
- National Science Foundation IGERT on Usable Privacy and Security, and CUPS

Questions/Feedback

David G. Gordon	Travis D. Breaux
dggordon@cmu.edu	breaux@cs.cmu.edu