Towards Regulatory Compliance: Extracting Rights and Obligation to Align Requirements with Regulations

Travis D. Breaux
Matthew W. Vail
Annie I. Antón
North Carolina State University

RE’06, Minneapolis, MN, USA, September 13th
Presentation Outline

- Regulations and Requirements
- Traceability in Legal Language
- Modeling Regulatory Semantics
- Case Study: HIPAA Privacy Rule
- Summary & Future Work
Problem Space: From Regulations to Requirements

- Regulations govern the system “environment.”
- Regulatory language is often complex and too ambiguous.
- Penalties for non-compliance can be severe:
  - HIPAA: up to $25K per individual, violation. (42 USC 160.404)
  - FCRA: historical civil fine of $10M and $5M in consumer redress (ChoicePoint, 2006); requires security audits every other year for 20 years.
  - SOX: up to $5M and 20 years in prison. (Title XI, Section 1106)
  - COPPA: historical civil fine of $1M. (Xanga.com, 2006)

... To be accountable, companies must demonstrate how their policies and system requirements align with regulations and standards.
Guidance for Lawyers and Engineers

- Develop a systematic method to extract high-level artifacts from regulations:
  - **Rights** describe what people are permitted to do.
  - **Obligations** describe what people are required to do.

- For each of these artifacts, we...
  - Identify relevant constraints.
  - Detect and resolve ambiguities.
  - Ensure traceability from regulations to requirements.

*Sounds easy enough?*
Traceability and Legal Language – 1

marking rights, obligations and constraints

(1) The covered entity who has a direct treatment relationship with the individual must...

(A) Provide notice no later than the first service delivery;

(2) For the purposes of paragraph (1), a covered entity who delivers services electronically must provide electronic notice unless the individual requests to receive a paper notice.

Obligations are red; Constraints are underlined; and Modal/ condition keywords are bold.

From HIPAA §160.520
(1) \([O_1]\) The covered entity \([C_1]\) who has a direct treatment relationship with the individual must...

(A) Provide notice \([C_2]\) no later than the first service delivery;

\(O_1: \) The covered entity must provide notice to the individual. (1)(A); \([C_1 \land C_2]\)

\(C_1: \) The covered entity has a direct treatment relationship with the individual. (1)

\(C_2: \) The notice is provided no later than the first service delivery. (A)
(2) For the purposes of paragraph (1), [\(O_2\)] a covered entity [\(C_3\)] who delivers services electronically must provide electronic notice unless [\(C_4\)] the individual requests to receive a paper notice.

\(O_2\): The covered entity must provide electronic notice to the individual. (2); \([C_1 \land C_2 \land C_3 \land \neg C_4]\)

\(C_3\): The covered entity delivers services electronically to the individual. (2)

\(C_4\): The individual requests to receive a paper notice. (2)
(1) \([O_1]\) The covered entity \([C_1]\) who has a direct treatment relationship with the individual must...

(A) Provide notice \([C_2]\) no later than the first service delivery;

(2) For the purposes of paragraph (1), \([O_2]\) a covered entity \([C_3]\) who delivers services electronically must provide electronic notice unless... \([C_4]\)

- From paragraph (1) we extracted \(O_1\): \([C_1 \land C_2]\)
- Now we carry down \(C_1, C_2\) from paragraph (1) to yield \(O_2\): \([C_1 \land C_2 \land C_3 \land \neg C_4]\)
O₁: The covered entity (CE) must provide notice to the individual.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Subject</th>
<th>Action</th>
<th>Object</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction</td>
<td>CE</td>
<td>provide</td>
<td>notice</td>
<td>individual</td>
</tr>
</tbody>
</table>

Z Notation:

\[ \exists v: \text{Activity}; s:\text{CE}; a: \text{Provide}; o: \text{Notice}; t: \text{Individual} \]
\[ \text{subject}(v, s) \land \text{action}(v, a) \land \text{object}(v, o) \land \text{target}(v, t) \]

Description Logic:

\[ \text{Activity} \sqsubseteq \text{hasSubject.} \text{CE} \sqsubseteq \text{hasAction.} \text{Provide} \sqsubseteq \]
\[ \text{hasObject.} \text{Notice} \sqsubseteq \text{hasTarget.} \text{Individual} \]
Case Study

The HIPAA Privacy Rule
Compliance Controversy?

HIPAA/PIPEDA/EU/OECD: Regulatory Compliance
Stiff criminal and civil penalties may be imposed for non-compliance. Our software fully complies with all current HIPAA regulations, as well as the Common ...
www.sona-systems.com/compliance.asp - 14k - Cached - Similar pages

HIPAA.ORG - EDI Practice Management System Directory
There is no such thing as "HIPAA compliant" software. The responsibility to be compliant rests with the practice. However, the software can be "HIPAA ready" ...
www.hipaa.org/pmsdirectory/help_physicians.php - 18k - Cached - Similar pages
## Analysis Results: An Overview

<table>
<thead>
<tr>
<th>Section Description</th>
<th>R</th>
<th>O</th>
<th>C</th>
<th>Refs</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.520: Notice of privacy practices</td>
<td>9</td>
<td>17</td>
<td>54</td>
<td>37</td>
</tr>
<tr>
<td>164.522: Requests to restrict access to health information</td>
<td>7</td>
<td>19</td>
<td>19</td>
<td>9</td>
</tr>
<tr>
<td>164.524: Access of individuals to health information</td>
<td>20</td>
<td>26</td>
<td>67</td>
<td>29</td>
</tr>
<tr>
<td>164.526: Amendment of health information</td>
<td>10</td>
<td>18</td>
<td>42</td>
<td>23</td>
</tr>
</tbody>
</table>

**KEY:** Rights (R); obligations (O); constraints (C); and cross-references (Refs) to other paragraphs.
## Normative Phrases - 1

<table>
<thead>
<tr>
<th>Phrase</th>
<th>N</th>
<th>Modality</th>
</tr>
</thead>
<tbody>
<tr>
<td>does not have a right to</td>
<td>1</td>
<td>Anti-Right</td>
</tr>
<tr>
<td>has a right to</td>
<td>7</td>
<td>Right</td>
</tr>
<tr>
<td>is not required to</td>
<td>3</td>
<td>Anti-Obligation</td>
</tr>
<tr>
<td>may</td>
<td>16</td>
<td>Right</td>
</tr>
<tr>
<td>may not</td>
<td>2</td>
<td>Obligation</td>
</tr>
<tr>
<td>must</td>
<td>39</td>
<td>Obligation</td>
</tr>
<tr>
<td>retains the right to</td>
<td>1</td>
<td>Right</td>
</tr>
</tbody>
</table>

*Anti-rights and anti-obligations state that a right or obligation does not exist.*
**Normative Phrases – 2**
delegating rights and obligations

<table>
<thead>
<tr>
<th>Phrase</th>
<th>N</th>
<th>Modality</th>
</tr>
</thead>
<tbody>
<tr>
<td>may deny</td>
<td>3</td>
<td>Right</td>
</tr>
<tr>
<td>may not require</td>
<td>1</td>
<td>Obligation</td>
</tr>
<tr>
<td>may require</td>
<td>4</td>
<td>Right</td>
</tr>
<tr>
<td>must deny</td>
<td>1</td>
<td>Obligation</td>
</tr>
<tr>
<td>must permit</td>
<td>13</td>
<td>Obligation</td>
</tr>
<tr>
<td>must request</td>
<td>1</td>
<td>Obligation</td>
</tr>
</tbody>
</table>

*Stakeholders have rights and obligations to assign rights and obligations to others.*
Stakeholder Classification Hierarchy

- Stakeholders must satisfy all of the obligations in their classification hierarchy.

Diagram:

- Individual
- Personal Representative
- Covered Entity
- Correctional Institution
- Inmate

Subcategories:
- Health Care Clearing House
- Health Plan
- Health Care Provider
- Licensed Health Care Professional
- Group Health Plan
- Health Insurance Issuer
- Health Maintenance Organization
Prioritizing Rights and Obligations

- **Right:** An individual has a right to adequate notice from the CE of the uses and disclosures of PHI. (a)(1)

- **Anti-Right:** An inmate does not have a right to notice from the CE of the uses and disclosures of PHI. (a)(1), (a)(3)

... If an inmate is also an individual, should they receive notice under the law?

- Two approaches to handle exceptions:
  - DeMorgan’s Law applied to constraints
  - Defeasible rules with defeaters
Comparing Rights and Obligations...

- $O_2$: The CE **must** provide the notice to any person or individual. (c)
- $O_8$: The HP **must** provide the notice to any person or individual. (c), (c)(1)(i)
- $O_4$: The GHP **is not required to** provide notice to any person. (a)(2)(iii)

Recall from the stakeholder hierarchy that:

From HIPAA §160.520
Hierarchies of Obligations

$O_7$: The CE must provide the notice to any person.

$O_{10}$: The HCP must provide notice to the individual.

$O_{13}$: The CE must provide electronic notice to the individual.

$O_8$: The HP must provide the notice to any person or individual.

$O_{14}$: The CE must provide a paper notice to the individual.

$O_{15}$: The HCP must automatically provide electronic notice to the individual.

$O_2$: The GHP must provide notice to any person.

$O_4$: The GHP is not required to provide the notice to any person.

From HIPAA §160.520
Detecting and Resolving Ambiguities

Activities have a **subject**, **action** and **object**.

Transactions have **target**
(e.g., with whom the action is performed)
- The CE must provide notice. *(to whom?)*

Verb phrases can masquerade as nouns
(e.g., denial means “to deny,” disclosure means “to disclose”)
- The individual may request an amendment from the CE.
  *(who amends what?)*
Detecting and Resolving Ambiguities

- Activities have a **subject**, **action** and **object**.

- Transactions have **target**
  (e.g., with whom the action is performed)
  - The CE must provide notice. (to whom?)

- Verb phrases can masquerade as nouns
  (e.g., denial means “to deny,” disclosure means “to disclose”)
  - The individual may request an amendment from the CE.
    (who amends what?)

*The formal models enable automatically detecting these ambiguities so that engineers can resolve them.*
Implied Rights and Obligations

deleations, provisions, purposes

- The CE requires the individual to request an amendment in writing.
  - Implied obligation: The individual must request an amendment in writing.

- The individual has a right to receive notice from the CE.
  - Implied obligation: The CE must provide the notice to the individual.

- The CE must post the notice for the individual to read.
  - Implied right: The individual has a right to read the notice.
Implied Rights and Obligations
delegations, provisions, purposes

- The CE requires the individual to request an amendment in writing.
  - Implied obligation: The individual must request an amendment in writing.

- The individual has a right to receive notice from the CE.
  - Implied obligation: The CE must provide the notice to the individual.

- The CE must post the notice for the individual to read.
  - Implied right: The individual has a right to read the notice.

Using formal models of rights and obligations, we can infer implies rights from obligations and vice versa.
In Summary…

- Systematic methodology to extract stakeholder rights and obligations from regulations.
  - Manage traceability and cross-referencing.
  - Multiple viewpoints from implied rights/obligations.
  - Techniques to compare, prioritize rights and obligations.
  - Detect and resolve ambiguities/under-specifications.

- Limitations
  - Applied to a narrow domain: information privacy.
  - The normative phrases are exhaustive.

- Current and Future Work
  - Evaluate the method with others, in other domains.
  - Derive software artifacts (the last mile).