Specifying policies in a formal language in order to automatically check for compliance

Lay Kuan Loh
Carnegie Mellon University
September 9, 2016
Projects

- Pick a group and topic for your class project
- Groups of 2 or 3
- List of topics on Piazza
- Talk to us if you want to propose your own topic
- Informal (non-graded) discussion of your proposal in class next week
- Graded presentations on your proposals on Monday, September 26
Homework 1

- Out next Monday, September 12
- You will use a tool to called REDUCE to check a hospital’s logs for compliance with HIPAA
- Due Wednesday, September 21
- *This is the one people have had the most trouble with in the past, so start early*
**Motivation**

Automatically audit the logs of organizations to check for compliance with governing policies

*Example Uses:*

- Auditing the activities logs in a hospital to ensure the practices comply with HIPAA
- TurboTax
Example: English to First-Order Logic

Identifying a potential criminal

A covered entity may disclose an individual’s protected health information to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participation in a violent crime that the covered entity believes may have caused serious physical harm to the victim.

<table>
<thead>
<tr>
<th>Type</th>
<th>Constant</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>( \phi )</td>
<td>protected health information</td>
</tr>
<tr>
<td>Role</td>
<td>official</td>
<td>law enforcement official</td>
</tr>
<tr>
<td>Purpose</td>
<td>id-criminal</td>
<td>identify a criminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Predicate</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>send((p_1, p_2, m))</td>
<td>( p_1 ) sends message ( m ) to ( p_2 )</td>
</tr>
<tr>
<td>tagged((m, q, t, u))</td>
<td>( m ) is a message containing information with attributes ( t ) about ( q ) with purpose ( u )</td>
</tr>
<tr>
<td>inrole((p_2, \text{official}))</td>
<td>( p_2 ) has the role of a law-enforcement-official</td>
</tr>
<tr>
<td>attr_in((t, I))</td>
<td>( t ) contains information ( I )</td>
</tr>
<tr>
<td>purp_in((u, \text{id-criminal}))</td>
<td>purpose ( u ) is identifying a criminal</td>
</tr>
<tr>
<td>state((q, s))</td>
<td>( q ) states ( s )</td>
</tr>
<tr>
<td>is-admission-of-crime((s))</td>
<td>( s ) is an admission of crime</td>
</tr>
<tr>
<td>believes-caused-harm((p_1, q, s))</td>
<td>( p_1 ) believes ( q ) may have caused serious harm</td>
</tr>
</tbody>
</table>
Example: English $\Rightarrow$ First-Order Logic

**Identifying a potential criminal**

A covered entity may disclose an individual’s protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participation in a violent crime that the covered entity believes may have caused serious physical harm to the victim.

\[
\forall p_1, p_2, m, q, t,
\begin{align*}
&\text{send}(p_1, p_2, m) \\
&\land \text{tagged}(m, q, t, u) \\
&\land \text{attr_in}(t, \text{phi}) \\
&\text{implies} \\
&\text{inrole}(p_1, \text{covered-entity}) \\
&\land \text{inrole}(p_2, \text{official}) \\
&\land \text{purp-in}(u, \text{id-criminal}) \\
&\land \exists s \text{ s.t.} \\
&\Diamond \text{state}(q, s) \\
&\land \text{is-admission-of-crime}(s) \\
&\land \text{believes-caused-harm}(p_1, q, s)
\end{align*}
\]

*Where $\Diamond$ denotes that the following happened in the past*
Reporting a crime

A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
(A) The commission and nature of a crime;
(B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime.

<table>
<thead>
<tr>
<th>Type</th>
<th>Constant</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>φ</td>
<td>protected health information</td>
</tr>
<tr>
<td>Role</td>
<td>provider official</td>
<td>health care provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>law enforcement official</td>
</tr>
</tbody>
</table>
| Purpose    | alert    | alert (someone) about
(A) The commission and nature of a crime;
(B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime |
Exercise: English to First-Order Logic

Reporting a crime

A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
(A) The commission and nature of a crime;
(B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime

<table>
<thead>
<tr>
<th>Predicate</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>providing-emergency-healthcare($p_1$, $q$)</td>
<td>$p_1$ is providing emergency healthcare to $q$</td>
</tr>
<tr>
<td>appears-necessary($p_1$, $p_2$, $q$, $t$, $u$)</td>
<td>$p_1$ thinks it necessary to alert $p_2$ with message $q$ with attribute $t$ for purpose $u$</td>
</tr>
<tr>
<td>send($p_1$, $p_2$, $m$)</td>
<td>$p_1$ sends message $m$ to $p_2$</td>
</tr>
<tr>
<td>tagged($m$, $q$, $t$, $u$)</td>
<td>$m$ is a message containing information with attributes $t$ about $q$ with purpose $u$</td>
</tr>
<tr>
<td>inrole($p_2$, $r$)</td>
<td>$p_2$ has the role $r$</td>
</tr>
<tr>
<td>attr_in($t$, $\phi$)</td>
<td>$t$ contains $\phi$</td>
</tr>
<tr>
<td>purp_in($u$, id-criminal)</td>
<td>purpose $u$ is identifying a criminal</td>
</tr>
</tbody>
</table>
A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;
(B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime

∀p₁, p₂, m, q, t,
    send(p₁, p₂, m)
∧tagged(m, q, t, u)
∧attr_in(t, phi)
implies
    inrole(p₁, health-care-provider)
∧inrole(p₂, law-enforcement-official)
∧purp-in(u, alert)
∧providing-emergency-healthcare(p₁, q)
∧appears-necessary(p₁, p₂, q, t, u)
Recap on norms in privacy laws

**Positive norms:** $\varphi^+$

If condition is satisfied, transmission *may occur.*

“A covered entity *may disclose* protected health information for treatment activities ...”

**Negative norms:** $\varphi^-$

If transmission occurs, condition *must be* satisfied.

“A covered entity *must obtain* an authorization for any use or disclosure of psychotherapy notes.”
Lawful transmission of confidential information

A transmission is lawful if an only if it satisfies at least one positive norm and all negative norms

\[ \text{maySend}(p_1, p_2, m) \triangleq (\bigvee \varphi^+) \land (\bigwedge \varphi^-) \]
Exercise: Combining the clauses

Identifying a potential criminal

A covered entity may disclose an individual’s protected health information ($\phi$) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participation in a violent crime that the covered entity believes may have caused serious physical harm to the victim.

Reporting a crime

A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;
(B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime

Note: Both clauses are positive norms
∀p₁, p₂, m, q, t,
 send(p₁, p₂, m)
 ∧ tagged(m, q, t, u)
 ∧ attr_in(t, phi)
 implies
 inrole(p₁, covered-entity)
 ∧ inrole(p₂, official)
 ∧ purp-in(u, id-criminal)
 ∧ ∃s s.t.
   ◊ state(q, s)
   ∧ is-admission-of-crime(s)
   ∧ believes-caused-harm(p₁, q, s)

∀p₁, p₂, m, q, t,
 send(p₁, p₂, m)
 ∧ tagged(m, q, t, u)
 ∧ attr_in(t, phi)
 implies
 inrole(p₁, health-care-provider)
 ∧ inrole(p₂, law-enforcement-official)
 ∧ purp-in(u, alert)
 ∧ providing-emergency-healthcare(p₁, q)
 ∧ appears-necessary(p₁, p₂, q, t, u)
∀p₁, p₂, m, q, t,
  send(p₁, p₂, m)
  ∧tagged(m, q, t, u)
  ∧attr_in(t, phi)
  implies
    (inrole(p₁, covered-entity)
     ∧inrole(p₂, official)
     ∧purp-in(u, id-criminal)
     ∧∃s s.t.
      ◊ state(q, s)
      ∧is-admission-of-crime(s)
      ∧believes-caused-harm(p₁, q, s)
    ) ∨
    (inrole(p₁, health-care-provider)
     ∧inrole(p₂, law-enforcement-official)
     ∧purp-in(u, alert)
     ∧providing-emergency-healthcare(p₁, q)
     ∧appears-necessary(p₁, p₂, q, t, u)
  )
## Exercise: English to First-Order Logic

### Reporting a death

A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

<table>
<thead>
<tr>
<th>Type</th>
<th>Constant</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>$\phi$</td>
<td>protected health information</td>
</tr>
<tr>
<td>Role</td>
<td>covered-entity</td>
<td>person/organization who must obey HIPAA</td>
</tr>
<tr>
<td></td>
<td>coroner</td>
<td>Coroner</td>
</tr>
<tr>
<td></td>
<td>medical-examiner</td>
<td>Medical examiner</td>
</tr>
<tr>
<td></td>
<td>deceased</td>
<td>a Deceased (person)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Function</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>identification($q$)</td>
<td>Identify who person $q$ is</td>
</tr>
<tr>
<td></td>
<td>determine-cause-of-death($q$)</td>
<td>determine the cause of death of person $q$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Predicate</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>is-authorized-by-law(p_2, u)</code></td>
<td>$p_2$ is authorized by law to carry out activities for purpose $u$</td>
</tr>
<tr>
<td><code>belongrole(q, (role))</code></td>
<td>$q$ has a role $role$</td>
</tr>
<tr>
<td><code>send(p_1, p_2, m)</code></td>
<td>$p_1$ sends message $m$ to $p_2$</td>
</tr>
<tr>
<td><code>tagged(m, q, t, u)</code></td>
<td>$m$ is a message containing information with attributes $t$ about $q$ with purpose $u$</td>
</tr>
<tr>
<td><code>inrole(p_2, (role))</code></td>
<td>$p_2$ has the role $role$</td>
</tr>
<tr>
<td><code>attr_in(t, \phi)</code></td>
<td>$t$ contains $\phi$ (protected health information)</td>
</tr>
<tr>
<td><code>purp_in(u, (purpose))</code></td>
<td>purpose $u$ is identifying a criminal</td>
</tr>
</tbody>
</table>
Answer: English to First-Order Logic

Reporting a death

A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

\[ \forall p_1, p_2, m, q, t, \]
\[ \text{send}(p_1, p_2, m) \]
\[ \land \text{tagged}(m, q, t, u) \]
\[ \land \text{attr}_\text{in}(t, \phi) \]
\[ \text{implies} \]
\[ ( \]
\[ \text{inrole}(p_1, \text{covered-entity}) \]
\[ \land (\text{inrole}(p_2, \text{coroner}) \lor \text{inrole}(p_2, \text{medical-examiner})) \]
\[ ) \]
\[ \land \text{belongtosrole}(q, \text{deceased}) \]
\[ \land ( \]
\[ \text{purp}_\text{in}(u, \text{identification}(q)) \]
\[ \lor \text{purp}_\text{in}(u, \text{determining-cause-of-death}(q)) \]
\[ \lor \text{authorized-by-law}(p_2, u) \]
\[ ) \]
## Notation: First-Order Logic vs REDUCE

<table>
<thead>
<tr>
<th>First-Order Logic</th>
<th>REDUCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a \land b$</td>
<td>(and (a) (b))</td>
</tr>
<tr>
<td>$a \lor b$</td>
<td>(or (a) (b))</td>
</tr>
<tr>
<td>$a + b$</td>
<td>(plus (a) (b))</td>
</tr>
<tr>
<td>$a - b$</td>
<td>(minus (a) (b))</td>
</tr>
<tr>
<td>$\forall x, y, c(x, y) \supset d(x, y)$</td>
<td>(all[x][y] (c(x,y)) (d(x,y)))</td>
</tr>
<tr>
<td>$\exists x, y, c(x, y) \land d(x, y)$</td>
<td>(ex[x][y] (c(x,y)) (d(x,y)))</td>
</tr>
<tr>
<td>$\exists x, y, c(x, y) \land d(x, y) \land e(x, y)$</td>
<td>(ex[x][y] (c(x,y)) (and (d(x,y)) (e(x,y))))</td>
</tr>
</tbody>
</table>

The encoding for existence in REDUCE only takes two arguments.
∀p₁, p₂, m, q, t,
 send(p₁, p₂, m)
 ∧ tagged(m, q, t, u)
 ∧ attr_in(t, phi)
 implies
 inrole(p₁, covered-entity)
 ∧ inrole(p₂, official)
 ∧ purp-in(u, id-criminal)
 ∧ ∃s s.t.
  ♦ state(q, s)
 ∧ is-admission-of-crime(s)
 ∧ believes-caused-harm(p₁, q, s)
Answer: First-Order Logic → REDUCE

\[
\begin{aligned}
&\text{all}[p1][p2][m][q][t] \\
&(\text{and} \\
&(\text{send}(p1,p2,m)) \\
&(\text{tagged}(m, q, t, u)) \\
&(\text{attrin}(t, \phi)) \\
&\text{)} \\
&(\text{and} \\
&(\text{inrole}(p1,\text{covered-entity})) \\
&(\text{inrole}(p2,\text{official})) \\
&(\text{purp-in}(u,\text{id-criminal})) \\
&(\text{ex } s \\
&(\text{state}(q,s)) \\
&(\text{and} \\
&(\text{is-admission-of-crime}(s)) \\
&(\text{believes-caused-harm}(p1,q,s)) \\
&\)) \\
&\text{)} \\
&\text{)}
\end{aligned}
\]
How to run REDUCE tool

all [p1][p2][m][i][p][t][u][pp]
  (and
    (send p1 p2 m u)
    (eq_msg m (msg i pp))
    (hasattrof i p t)
  )
(ex[u1]
  (inrelation p1 p treatment-relation u1)
  (time_in (plus u 30) u1 u)
)