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 acitivites logs in a hospital to ensure the practices comply with HIPAA
- TurboTax

Example: English to First-Order Logic

Identifiying 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.

Type	Constant	English
Information	ϕ	protected health information
Role	*official*	law enforcement official
Purpose	*id-criminal*	identify a criminal

Predicate	English
`send`(p_1, p_2, m)	p_1 sends message m to p_2
`tagged`(m, q, t, u)	m is a message containing information with attributes t about q with purpose u
`inrole`$(p_2, \textit{official})$	p_2 has the role of a law-enforcement-official
`attr_in`$(t, \mathcal{I})$	t contains information $\mathcal{I}$
`purp_in`$(u, \textit{id-criminal})$	purpose u is identifying a criminal
`state`(q, s)	q states s
`is-admission-of-crime`(s)	s is an admission of crime
`believes-caused-harm`(p_1, q, s)	p_1 believes q may have caused serious harm

Example: English ⇒ First-Order Logic

Identifiying 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.

$\forall p_1, p_2, m, q, t,$
  $\texttt{send}(p_1, p_2, m)$
  $\wedge \texttt{tagged}(m, q, t, u)$
  $\wedge \texttt{attr\_in}(t, phi)$
  implies
    $\texttt{inrole}(p_1, \textit{covered-entity})$
    $\wedge \texttt{inrole}(p_2, \textit{official})$
    $\wedge \texttt{purp-in}(u, \textit{id-criminal})$
    $\wedge \exists s$ s.t.
      $\not\Diamond \texttt{state}(q, s)$
      $\wedge \texttt{is-admission-of-crime}(s)$
      $\wedge \texttt{believes-caused-harm}(p_1, q, s)$

Where $\not\Diamond$ denotes that the following happened in the past

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

Type	Constant	English
Information	ϕ	protected health information
Role	*provider* *official*	health care provider law enforcement official
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

Predicate	English
providing-emergency-healthcare(p_1, q)	p_1 is providing emergency healthcare to q
appears-necessary(p_1, p_2, q, t, u)	p_1 thinks it necessary to alert p_2 with message q with attribute t for purpose u
send(p_1, p_2, m)	p_1 sends message m to p_2
tagged(m, q, t, u)	m is a message containing information with attributes t about q with purpose u
inrole(p_2, r)	p_2 has the role r
attr_in(t, ϕ)	t contains ϕ
purp_in(u, *id-criminal*)	purpose u is identifying a criminal

Answer: 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

$$
\begin{aligned}
&\forall p_1, p_2, m, q, t, \\
&\quad \texttt{send}(p_1, p_2, m) \\
&\quad \wedge \texttt{tagged}(m, q, t, u) \\
&\quad \wedge \texttt{attr\_in}(t, \mathit{phi}) \\
&\quad \text{implies} \\
&\qquad \texttt{inrole}(p_1, \mathit{health\text{-}care\text{-}provider}) \\
&\qquad \wedge \texttt{inrole}(p_2, \mathit{law\text{-}enforcement\text{-}official}) \\
&\qquad \wedge \texttt{purp-in}(u, \mathit{alert}) \\
&\qquad \wedge \texttt{providing-emergency-healthcare}(p_1, q) \\
&\qquad \wedge \texttt{appears-necessary}(p_1, p_2, q, t, u)
\end{aligned}
$$

Recap on norms in privacy laws

Positive norms: φ^+

If condition is satisfied, transmission *may occur.*

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

Negative norms: φ^-

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

$$\texttt{maysend}(p_1, p_2, m) \triangleq \left(\bigvee \varphi^+\right) \wedge \left(\bigwedge \varphi^-\right)$$

Exercise: Combining the clauses

Identifiying a potential criminal

A covered entity may disclose an individual's protected health information (ϕ) 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

Exercise: English ⇒ First-Order Logic

$\forall p_1, p_2, m, q, t,$
$\quad \texttt{send}(p_1, p_2, m)$
$\quad \wedge \texttt{tagged}(m, q, t, u)$
$\quad \wedge \texttt{attr\_in}(t, phi)$
$\quad$ implies
$\quad\quad \texttt{inrole}(p_1, \textit{covered-entity})$
$\quad\quad \wedge \texttt{inrole}(p_2, \textit{official})$
$\quad\quad \wedge \texttt{purp-in}(u, \textit{id-criminal})$
$\quad\quad \wedge \exists s$ s.t.
$\quad\quad\quad \diamondminus\, \texttt{state}(q, s)$
$\quad\quad\quad \wedge \texttt{is-admission-of-crime}(s)$
$\quad\quad\quad \wedge \texttt{believes-caused-harm}(p_1, q, s)$

$\forall p_1, p_2, m, q, t,$
$\quad \texttt{send}(p_1, p_2, m)$
$\quad \wedge \texttt{tagged}(m, q, t, u)$
$\quad \wedge \texttt{attr\_in}(t, phi)$
$\quad$ implies
$\quad\quad \texttt{inrole}(p_1, \textit{health-care-provider})$
$\quad\quad \wedge \texttt{inrole}(p_2, \textit{law-enforcement-official})$
$\quad\quad \wedge \texttt{purp-in}(u, \textit{alert})$
$\quad\quad \wedge \texttt{providing-emergency-healthcare}(p_1, q)$
$\quad\quad \wedge \texttt{appears-necessary}(p_1, p_2, q, t, u)$

Answer: English ⇒ First-Order Logic

$$
\begin{array}{l}
\forall p_1, p_2, m, q, t, \\
\quad \texttt{send}(p_1, p_2, m) \\
\quad \wedge \texttt{tagged}(m, q, t, u) \\
\quad \wedge \texttt{attr\_in}(t, \mathit{phi}) \\
\quad \text{implies} \\
\quad\quad (\\
\quad\quad\quad \texttt{inrole}(p_1, \mathit{covered\text{-}entity}) \\
\quad\quad\quad \wedge \texttt{inrole}(p_2, \mathit{official}) \\
\quad\quad\quad \wedge \texttt{purp-in}(u, \mathit{id\text{-}criminal}) \\
\quad\quad\quad \wedge \exists s \text{ s.t.} \\
\quad\quad\quad\quad \diamondsuit\, \texttt{state}(q, s) \\
\quad\quad\quad\quad \wedge \texttt{is-admission-of-crime}(s) \\
\quad\quad\quad\quad \wedge \texttt{believes-caused-harm}(p_1, q, s) \\
\quad\quad) \\
\quad\quad \vee \\
\quad\quad (\\
\quad\quad\quad \texttt{inrole}(p_1, \mathit{health\text{-}care\text{-}provider}) \\
\quad\quad\quad \wedge \texttt{inrole}(p_2, \mathit{law\text{-}enforcement\text{-}official}) \\
\quad\quad\quad \wedge \texttt{purp-in}(u, \mathit{alert}) \\
\quad\quad\quad \wedge \texttt{providing-emergency-healthcare}(p_1, q) \\
\quad\quad\quad \wedge \texttt{appears-necessary}(p_1, p_2, q, t, u) \\
\quad\quad)
\end{array}
$$

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 deceases person, determining a cause of death, or other duties as authorized by law.

Type	Constant	English
Information	ϕ	protected health information
Role	*covered-entity*	person/organization who must obey HIPAA
	coroner	Coroner
	medical-examiner	Medical examiner
	deceased	a Deceased (person)

Type	Function	English
Purpose	`identification`(q)	Identify who person q is
	`determine-cause-of-death`(q)	determine the cause of death of person q

Predicate	English
`is-authorized-by-law`(p_2, u)	p_2 is authorized by law to carry out activites for purpose u
`belongrole`(q, $\langle role \rangle$)	q has a role *role*
`send`(p_1, p_2, m)	p_1 sends message m to p_2
`tagged`(m, q, t, u)	m is a message containing information with attributes t about q with purpose u
`inrole`(p_2, $\langle role \rangle$)	p_2 has the role *role*
`attr_in`(t, ϕ)	t contains ϕ (protected health information)
`purp_in`(u, $\langle purpose \rangle$)	purpose u is identifying a criminal

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 deceases person, determining a cause of death, or other duties as authorized by law

$$
\begin{aligned}
&\forall p_1, p_2, m, q, t, \\
&\quad \texttt{send}(p_1, p_2, m) \\
&\quad \wedge \texttt{tagged}(m, q, t, u) \\
&\quad \wedge \texttt{attr\_in}(t, \phi) \\
&\quad \text{implies} \\
&\qquad (\\
&\qquad\quad \texttt{inrole}(p_1, \textit{covered-entity}) \\
&\qquad\quad \wedge (\texttt{inrole}(p_2, \textit{coroner}) \vee \texttt{inrole}(p_2, \textit{medical-examiner}))) \\
&\qquad) \\
&\qquad \wedge \texttt{belongstorole}(q, \textit{deceased}) \\
&\qquad \wedge (\\
&\qquad\quad \texttt{purp-in}(u, \texttt{identification}(q)) \\
&\qquad\quad \vee \texttt{purp-in}(u, \texttt{determining-cause-of-death}(q)) \\
&\qquad\quad \vee \texttt{authorized-by-law}(p_2, u) \\
&\qquad\quad) \\
&\qquad\quad)
\end{aligned}
$$

Notation: First-Order Logic vs REDUCE

First-Order Logic	REDUCE
$a \wedge b$	(and (a) (b))
$a \vee b$	(or (a) (b))
$a + b$	(plus (a) (b))
$a - b$	(minus (a) (b))
$\forall x, y,\ c(x, y) \supset d(x, y)$	(all[x][y] (c(x,y)) (d(x,y)))
$\exists x, y,\ c(x, y) \wedge d(x, y)$	(ex[x][y] (c(x,y)) (d(x,y)))
$\exists x, y,\ c(x, y) \wedge d(x, y) \wedge e(x, y)$	(ex[x][y] (c(x,y)) (and (d(x,y)) (e(x,y)))

The encoding for existence in REDUCE only takes two arguments

Exercise: First-Order Logic → REDUCE

$$
\begin{aligned}
&\forall p_1, p_2, m, q, t, \\
&\quad \texttt{send}(p_1, p_2, m) \\
&\quad \wedge \texttt{tagged}(m, q, t, u) \\
&\quad \wedge \texttt{attr\_in}(t, \mathit{phi}) \\
&\quad \text{implies} \\
&\qquad \texttt{inrole}(p_1, \mathit{covered\text{-}entity}) \\
&\qquad \wedge \texttt{inrole}(p_2, \mathit{official}) \\
&\qquad \wedge \texttt{purp-in}(u, \mathit{id\text{-}criminal}) \\
&\qquad \wedge \exists s \text{ s.t.} \\
&\qquad\quad \diamondsuit\, \texttt{state}(q, s) \\
&\qquad\quad \wedge \texttt{is-admission-of-crime}(s) \\
&\qquad\quad \wedge \texttt{believes-caused-harm}(p_1, q, s)
\end{aligned}
$$

Answer: First-Order Logic → REDUCE

```
all[p1][p2][m][q][t]
   (and
      (send(p1,p2,m))
      (tagged(m, q, t, u))
      (attrin(t, phi))
   )
   (and
      (inrole(p1,covered-entity))
      (inrole(p2,official))
      (purp-in(u,id-criminal))
      (ex s
           (state(q,s))
           (and
              (is-admission-of-crime(s))
              (believes-caused-harm(p1,q,s))
           )
      )
   )
```

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)
   )
```