Legal Compliance, Privacy and Security

Travis D. Breaux
Assistant Professor of Computer Science
Institute for Software Research
Carnegie Mellon University

Presented at CMU Privacy Series, November 19, 2010

What's to come…

- Problem and Motivation
- Background and Related Work
- Legal Requirements Acquisition
- Empirical Validation
  - Case Studies
  - Experiments
- Contributions and Future Work

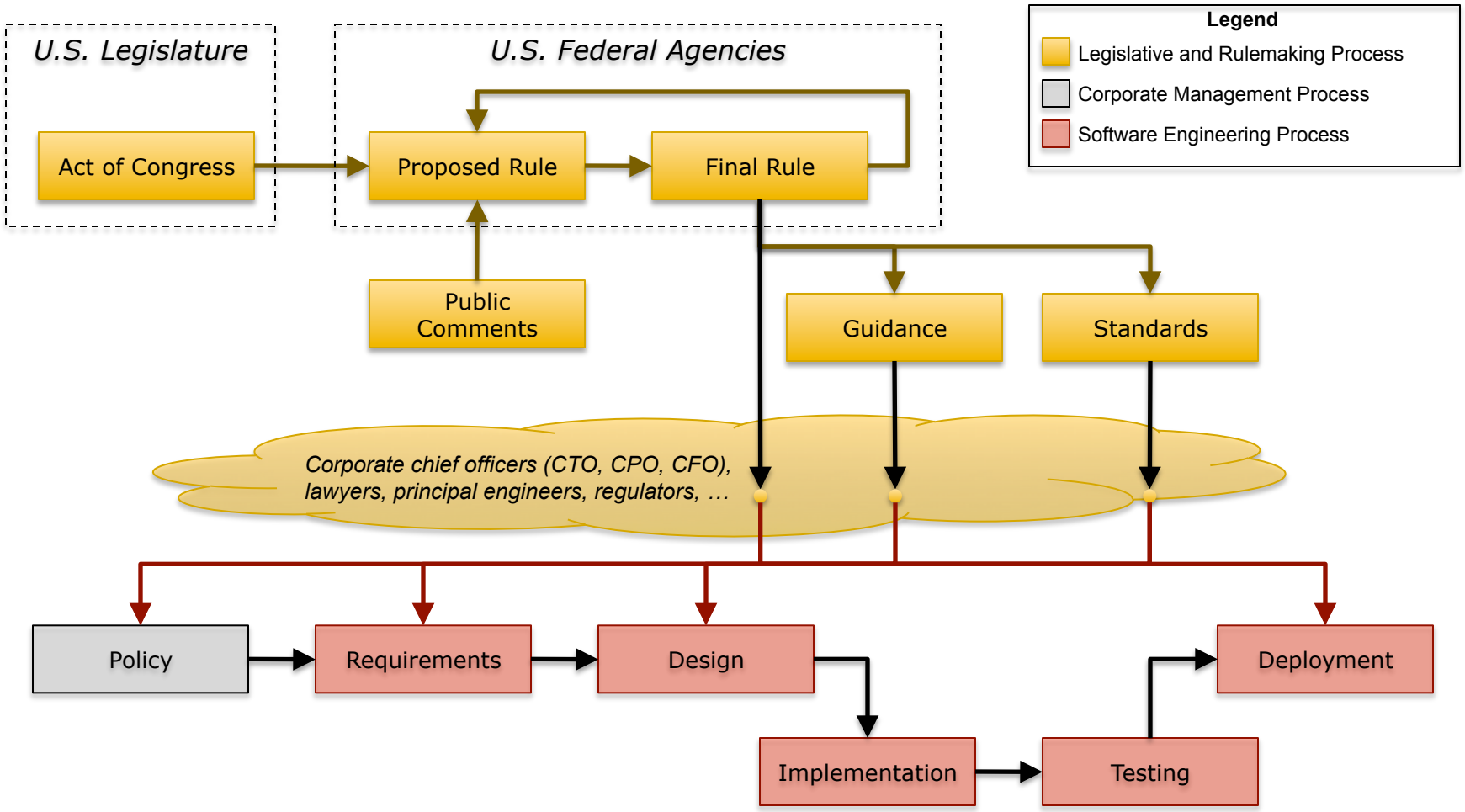
Compliance Problem

Organizations must ensure their information systems comply with privacy and security law.

Software engineers and system administrators must:

- Identify relevant legal requirements from policies, laws and regulations; and
- Align these requirements with system specifications

What do we mean by the law?



Why should computer scientists study the law?

The costs of non-compliance can be severe

- Civil fines and consumer redress:
  - ChoicePoint fined $15M for FCRA violations
  - CVS fined $2.25M for HIPAA violations
- Public harms: Over 14M consumers affected unfair and deceptive trade practices in 1999-08 *[Breaux and Baumer, 2009]*
- Reengineering: ChoicePoint spends $3M to update business and system processes *[Otto and Antón, 2007]*
- Legal fees and Consumer Churn

Legal Terminology

Due Diligence refers to reasonable efforts to satisfy legal requirements or discharge legal obligations

Good Faith includes observance of reasonable commercial standards of fair dealing in a given trade or business, or absence of intent to defraud or to seek unconscionable advantage

Standard of Care includes giving attention both to possible dangers, mistakes and pitfalls and to ways of minimizing those risks

[Black's Law Dictionary, 8th Ed.]

Legal Requirements Acquisition

Identifying Legal Requirements

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**…

Key:

Obligations are red
Constraints are underlined
Modal/ condition keywords are **bold**

Excerpt from HIPAA §160.520(c)

Extracting Legal Requirements

rights, obligations and constraints

(1) [O_1] The covered entity [C_1] who has a direct treatment relationship with the individual **must**…

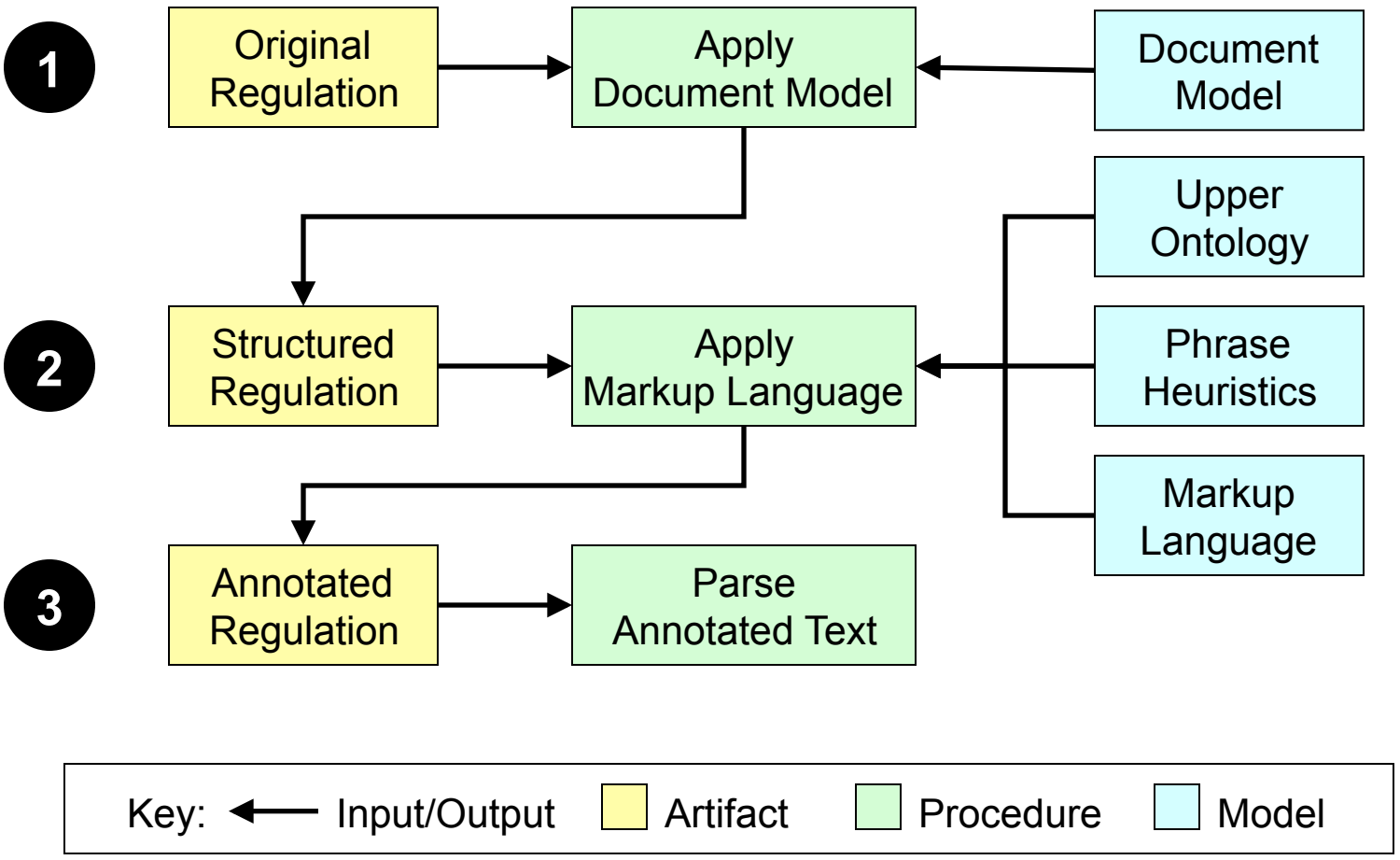
  (A) Provide notice [C_2] no later than the first service delivery;

(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: [$C_1 \wedge C_2$]
- Now we carry down C_1, C_2 from paragraph (1) to yield
  O_2: [$C_1 \wedge C_2 \wedge C_3 \wedge \neg C_4$]

Excerpt from HIPAA §160.520(c)

The Acquisition Method



Regulatory Document Model
XML Markup

```
<document>
  <!-- 164.520(a)(2)(i)(B) -->
  <div index="(ii)">
    A group health…, must:
    <div index="(A)">
      Maintain a notice under this section; and
    </div>
    <div index="(B)">
      Provide such notice to any person…
    </div>
    …
  </div><!-- end of (ii) -->
</document>
```

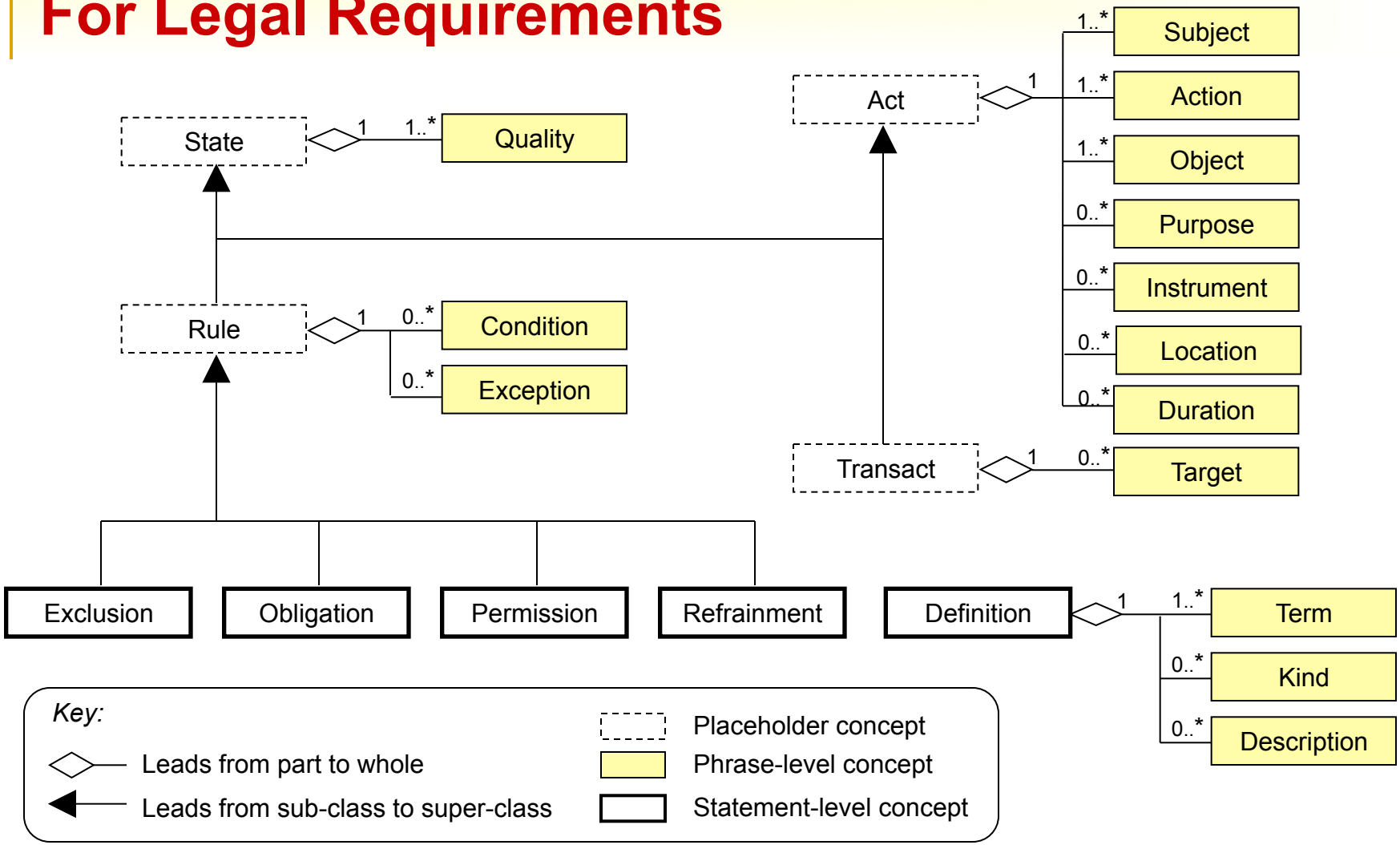
Types of Legal Statements

Statements about actions that a stakeholder or product is…

- Permitted to perform (***Permission***)
- Required to perform (***Obligation***)
- Prohibited from performing (***Refrainment***)
- Not expressly permitted or required to perform (***Exclusion***)
  (also called No-rights and Privileges by Hohfeld)

Definition is a statement that restricts the meaning of a term by one or more constraints

Standard Upper Ontology
For Legal Requirements



Phrase Heuristics

[IEEE RE 2006]

From HIPAA Privacy Rule §164.520-164.526:

Phrase Pattern	Concept
if	Condition
when	Condition
except when	Exception
is not required to	Exclusion
must	Obligation
*must deny**	Obligation
*must permit**	Obligation

Phrase Pattern	Concept
*must request**	Obligation
has a right to	Permission
may	Permission
*may deny**	Permission
*may require**	Permission
may not	Refrainment
*may not require**	Refrainment

* *these patterns denote delegations from one actor to another*

Types of Legal Ambiguity

- Logical ambiguity, words with different logical meanings
- Attributive ambiguity, phrases can be ascribed to multiple, other phrases
- Referential ambiguity, multiple extensional and intensional meanings, called polysemy
- Omissions and under-specifications

The notice must include "the name or title and telephone number of a person or office"

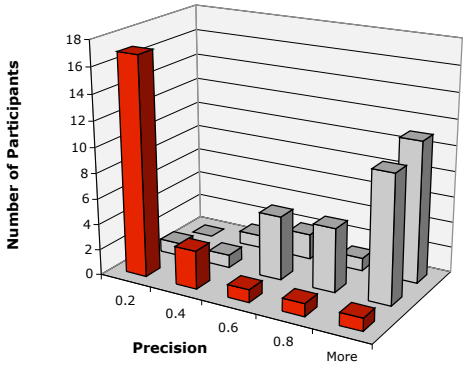
1. Name of a person or office?
2. Name and telephone number of a person or office?
3. Title and telephone number of a person or office?

Excerpt from HIPAA §160.520(b)(1)(vii)

Variance in Traditional Practice

89 Total Requirements Acquired

- Constraint integration and case splitting (17 of 89)
- Omissions and under-specifications (72 of 89)
- Changes in modality (50 of 89):
  - Balancing rights and obligations (32 of 89)
    e.g., must provide → may receive
  - Exclusions become refrainments (8 of 89)
    e.g., does not have a right to → shall not have a right to
  - Obligations changed to implied permissions (5 of 89)
    e.g., must → shall be able to



Classification Exercise Results

Over 94 responses per requirement type

- People more often (78% vs. 67%) correctly classify permissions that describe stakeholder rights
- Most people (68%) correctly classify obligations
  - 30% mislabel "shall allow" as a permission
- Most people (47%) correctly classify refrainments
  - 23% mislabel refrainments as exclusions
  - 23% mislabel "shall not" as an obligation
- Most people (55%) correctly classify exclusions
  - 31% mislabel exclusions as refrainments

Case Study Findings

Iterative Refinement of Theory

Formative Studies

- Goals: Most frequent 100 goals from over 100 Internet privacy policies *[POLICY'05, RE'05]*
- Facts: HIPAA Patient Fact Sheet from HHS *[WPES'05]*

Summative Case Studies

- Practices: HIPAA Privacy Rule (4 sections) *[RE'06, TOSEM'08]*
- Privacy: HIPAA Privacy Rule (entire rule) *[TSE'08]*
- Accessibility: Access Standards *[RE'08]*

Conducted using case study designs [Yin, 2003; Creswell, 2002]

Balancing Rights and Obligations

Practices Case Study #3

[IEEE RE 2006]

- Delegation - The covered entity (CE) may require the individual to request an amendment in writing
  - **(implied obligation)** The individual must request an amendment in writing
- Purposes and Conditions - The CE must post the notice for the individual to read
  - **(implied right)** The individual has a right to read the notice
- Transaction - The individual may receive notice from the CE
  - **(implied obligation)** The CE must provide notice to the individual

Beliefs and Determinations

Privacy Case Study #4

[IEEE TSE, January 2008]

Identified 300 data access requirements and 1894 constraints, including:

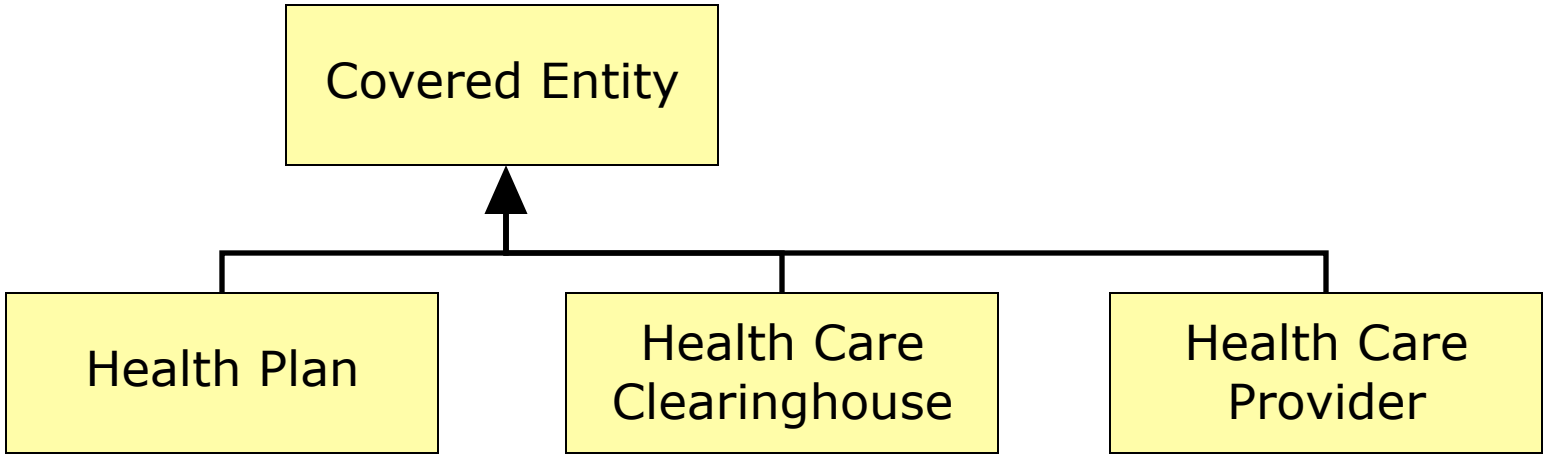
- Legal: Who is authorized by law to receive reports of child abuse or neglect
- Medical: Who determines the individual is incapacitated
- Personal: Who determines the consent of the individual is inferred from the circumstances
- Contractual: Who obtains an alteration or waiver of an individual's required authorization

Stakeholder Hierarchy

Practices Case Study #3

[IEEE RE 2006 / IEEE TSE, January 2008]

HIPAA §160.103: Covered entity means: a health plan, a health care clearinghouse and a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

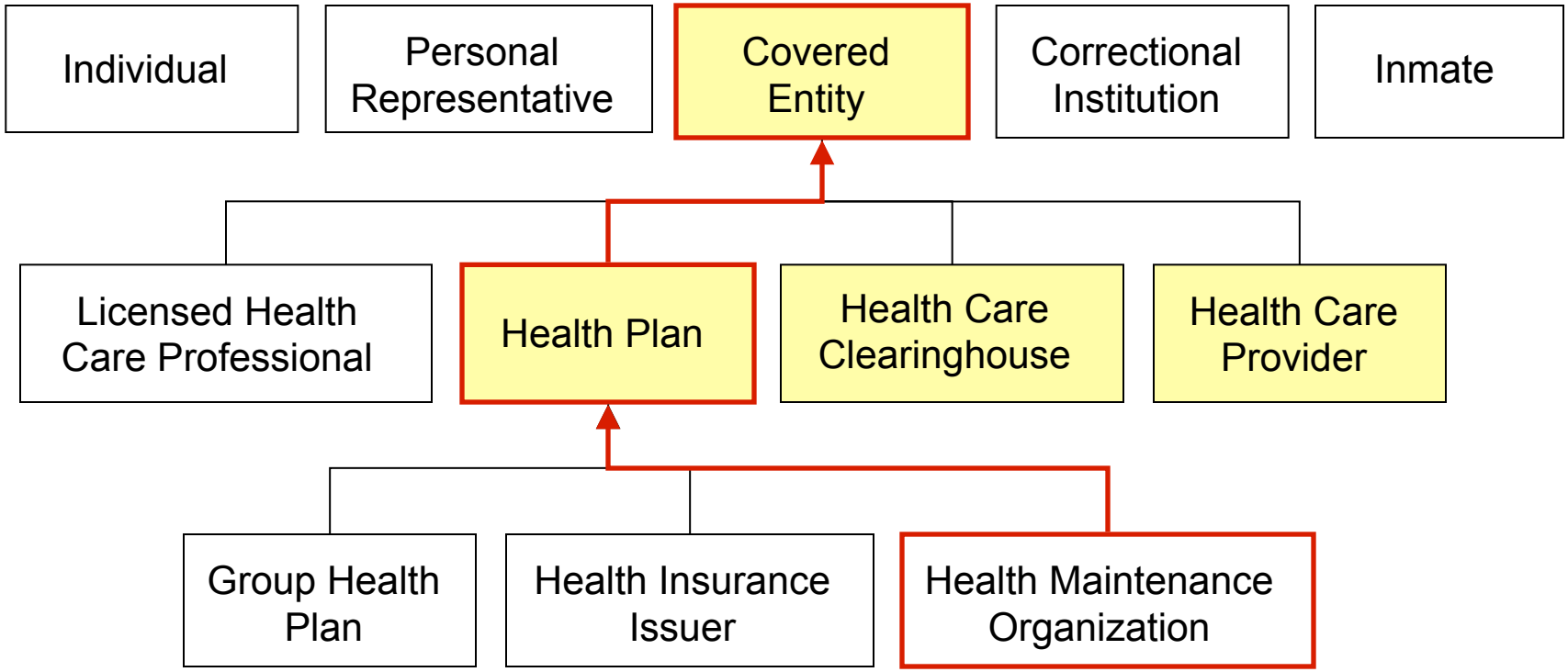


Key: ← Leads from sub-class to super-class

Stakeholder Hierarchy

Practices Case Study #3

[IEEE RE 2006 / IEEE TSE, January 2008]



Stakeholders must satisfy all of the obligations in their role hierarchy

Formalization in Logic

Obligation: The covered entity (CE) must provide notice to the individual.

Activity	***Subject***	***Action***	***Object***	***Target***
Transaction	CE	provide	notice	individual

Z Notation:

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

Description Logic:

$$Activity \sqcap hasSubject.CE \sqcap hasAction.Provide \sqcap$$
$$hasObject.Notice \sqcap hasTarget.Individual$$

Obligations with Subtle Differences

Practices Case Study #3

[ACM TOSEM, October 2008]

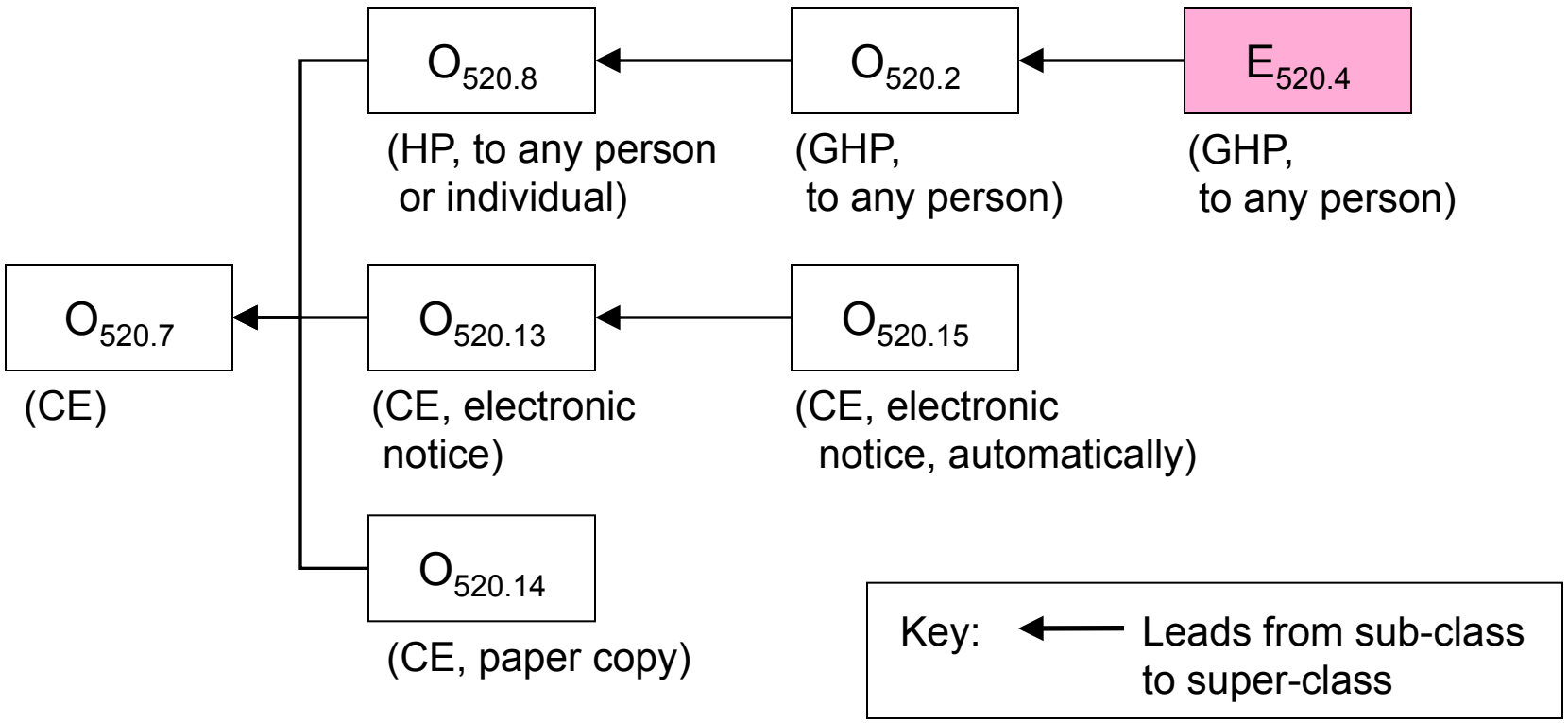
ID	Obligation Description
$O_{520.2}$	The GHP must provide notice to every person
$E_{520.4}$	The GHP is not required to provide notice to any person
$O_{520.7}$	The CE must provide notice to any person or individual
$O_{520\text{-}8}$	The HP must provide notice to any person or individual
$O_{520.10}$	The HCP must provide notice to the individual
$O_{520.13}$	The CE must provide electronic notice to the individual
$O_{520.14}$	The CE must provide a paper copy of the notice to the individual
$O_{520.15}$	The CE must automatically provide electronic notice to the individual

Requirement Specialization

Practices Case Study #3

[ACM TOSEM, October 2008]

Obligations to provide different types of notice to different actors



Visualizing Finite State Machines

[RELAW 2010]

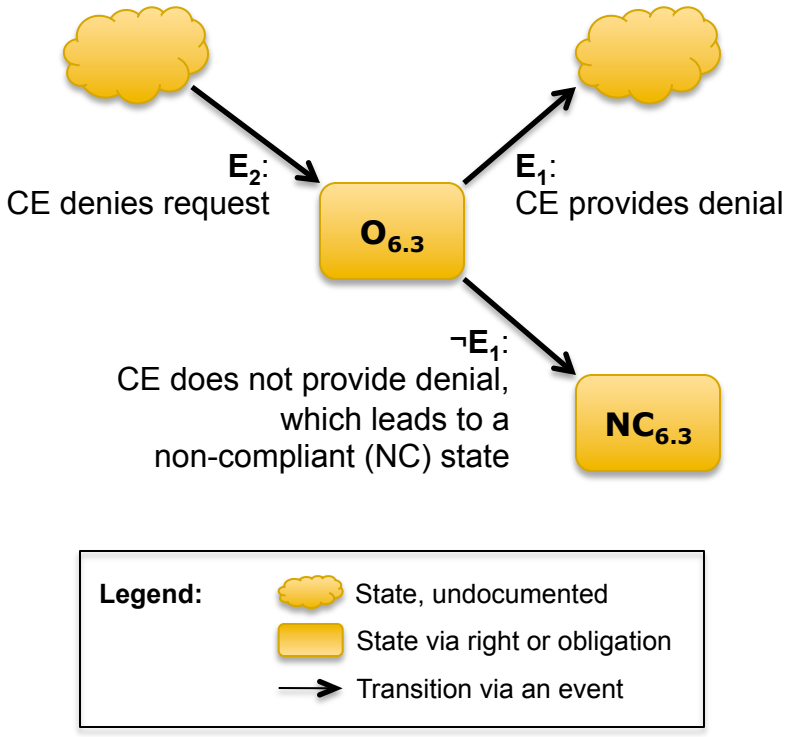
State-Event Table

Index	Subject	Action	Object
$O_{6.3}$	Rule	require	E_1
E_1	CE	provide	E_2
E_2	CE	deny	E_3
E_3	Individual	request	E_4
E_4	CE	amend	PHI

Transition Table

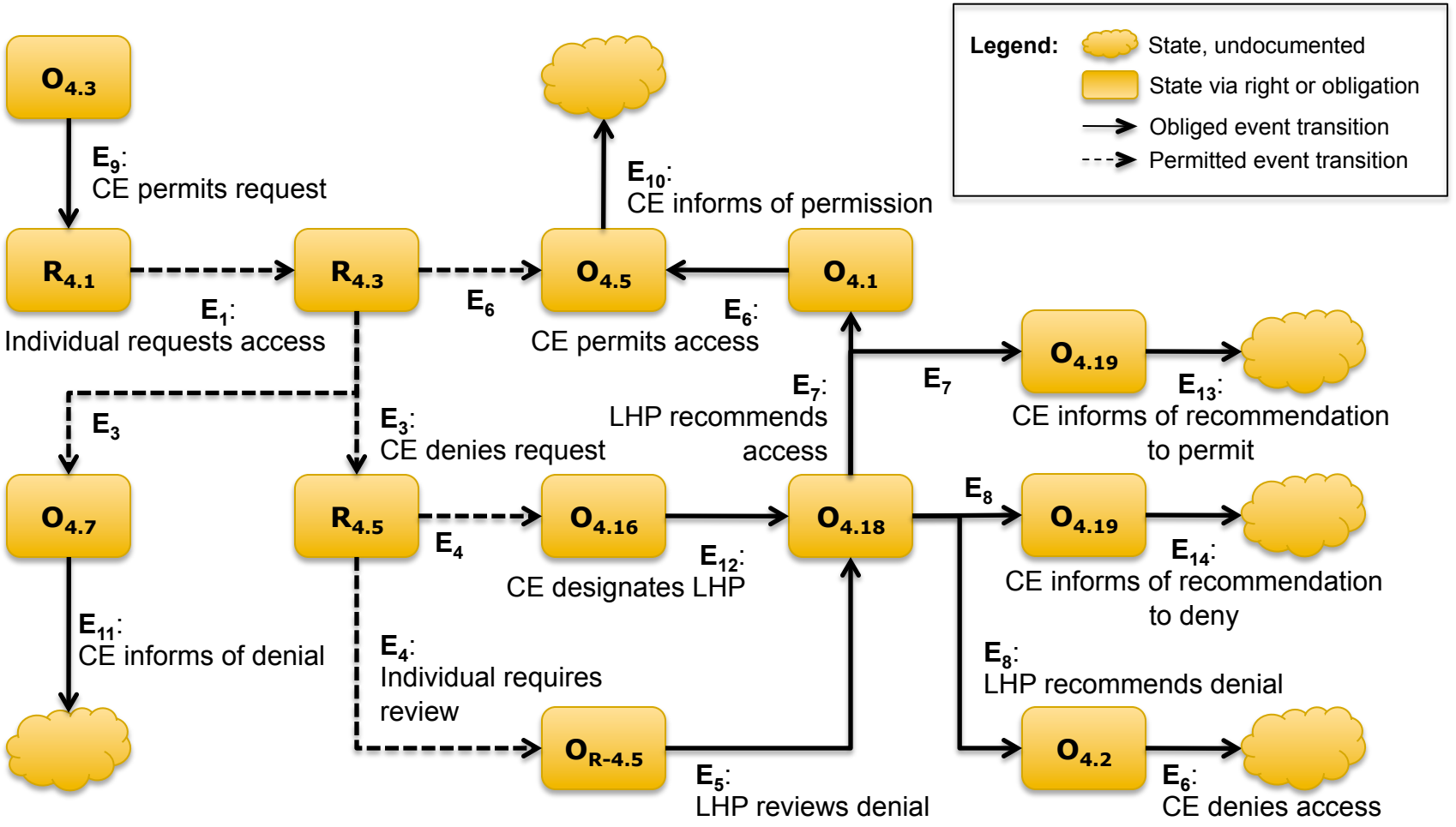
Set	Source	Event	Target
1		E_2	$O_{6.3}$
2	$O_{6.3}$	E_1	
3	$O_{6.3}$	$\neg E_1$	$NC_{6.3}$

Visualized Finite State Machine



Combined Compliance Monitor

Acquired from HIPAA Privacy Rule §164.524

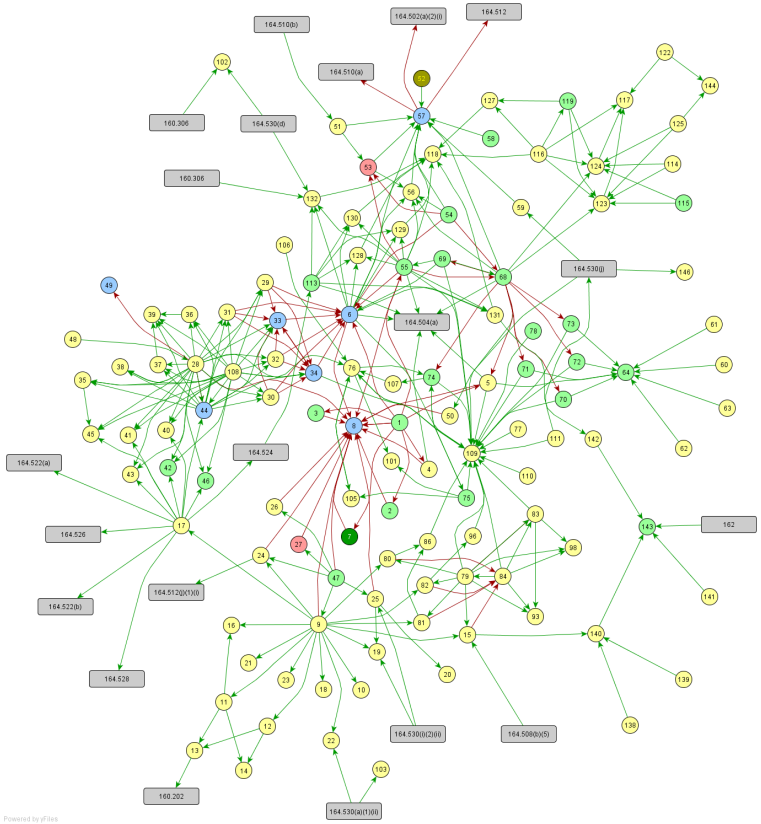


Carnegie Mellon

Interpreting Cross-references

Practices Case Study #3

- Identified 1720 mappings among legal requirements
- Cross-references types:
  - As defined in… (58%)
  - Except for… (36%)
  - As follows… (8%)
- 63% of requirements in referenced paragraphs were false-positive
- 52% of referenced requirements contain cross-references



Cross-reference graph acquired from HIPAA §164.520-526

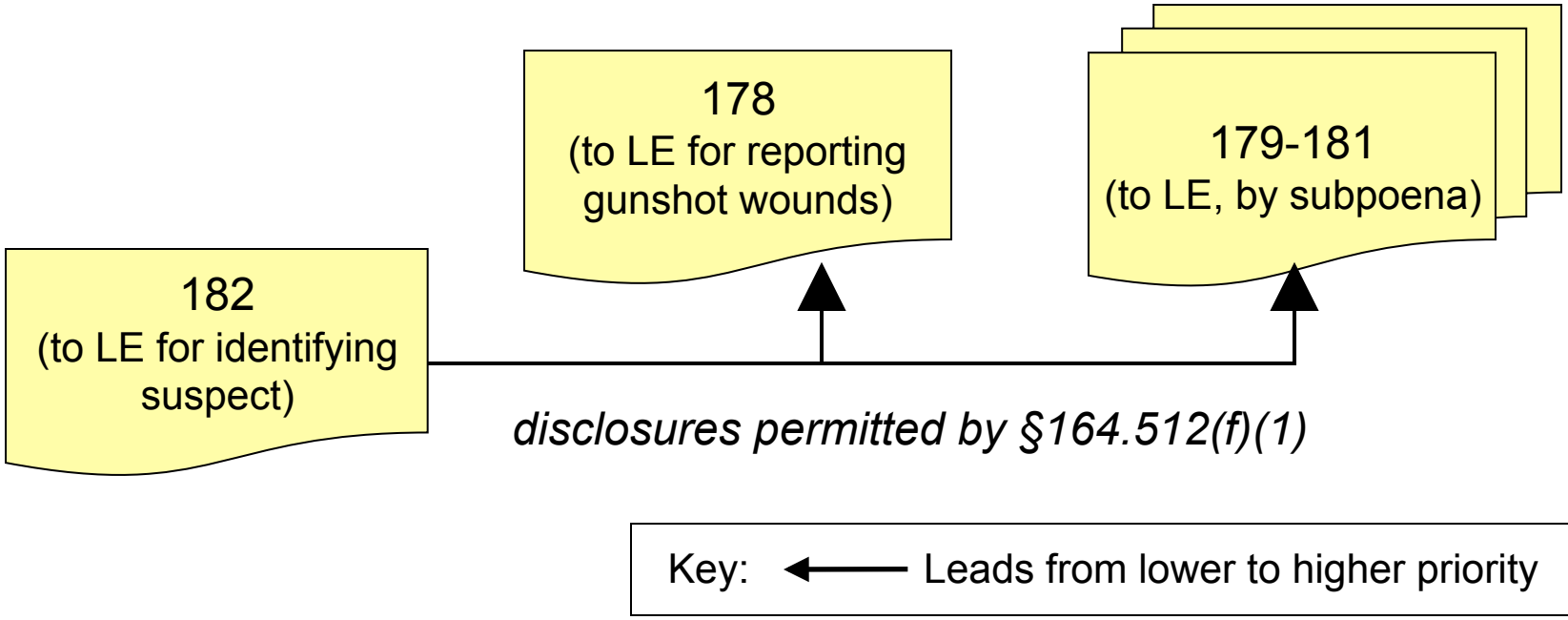
Carnegie Mellon

Handling Legal Exceptions

Privacy Case Study #4

[IEEE TSE, January 2008]

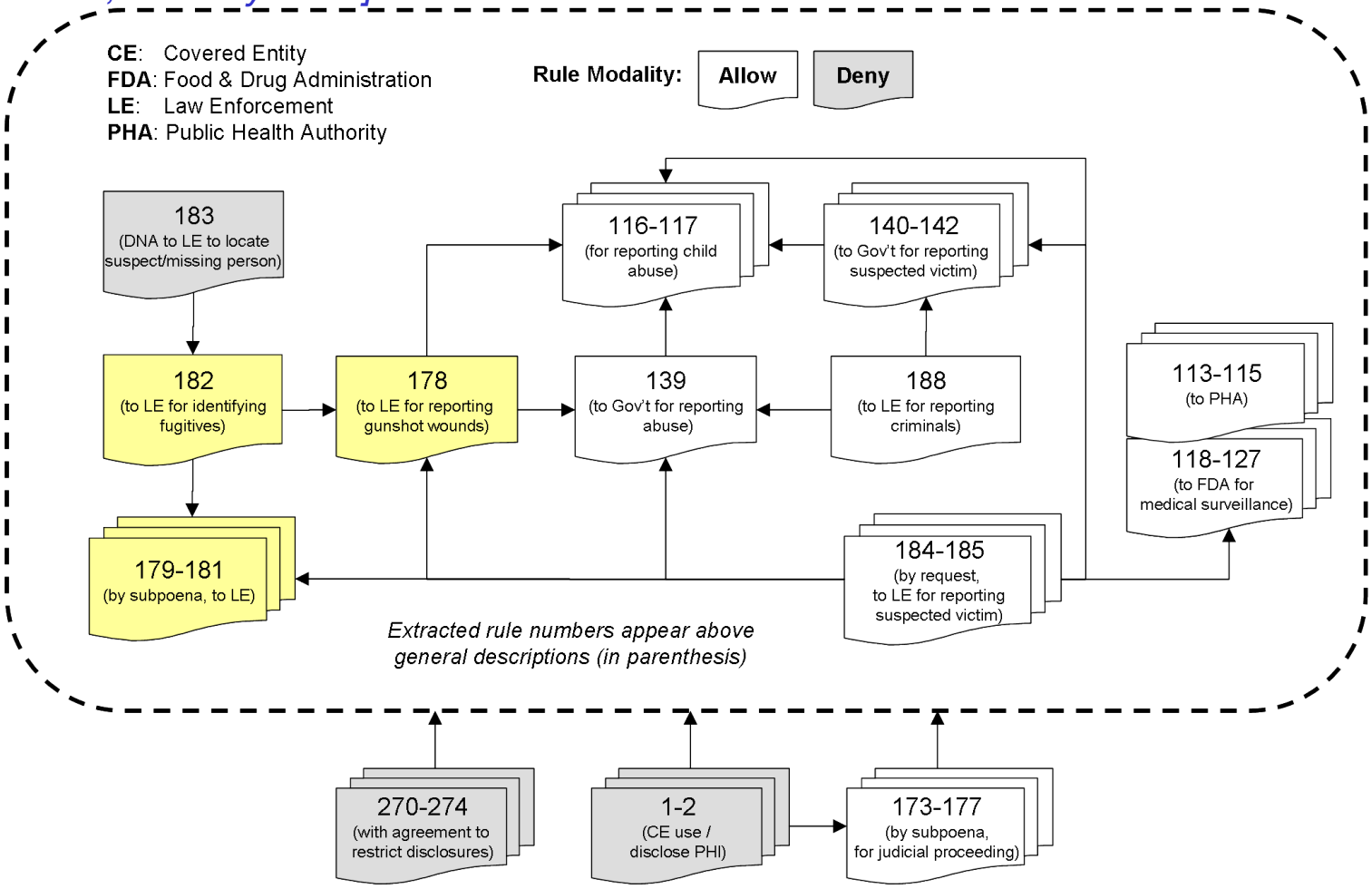
HIPAA §164.512(f)(2): Except for disclosures required by law as permitted by paragraph 164.512(f)(1), a CE may disclose PHI in response to a law enforcement (LE) official's request for the purpose of identifying or locating a suspect



Requirements Exception Hierarchy

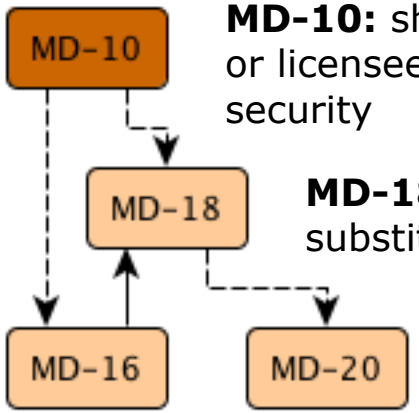
Privacy Case Study #4

[IEEE TSE, January 2008]



Conditional Surface Structure

- **Surface** consists of the "first-contact" conditions for an organization
- **Extension** consists of rules that refine or follow other rules



MD-10: shall notify owner or licensee of a breach of security

MD-18: may give notice by substitute notice

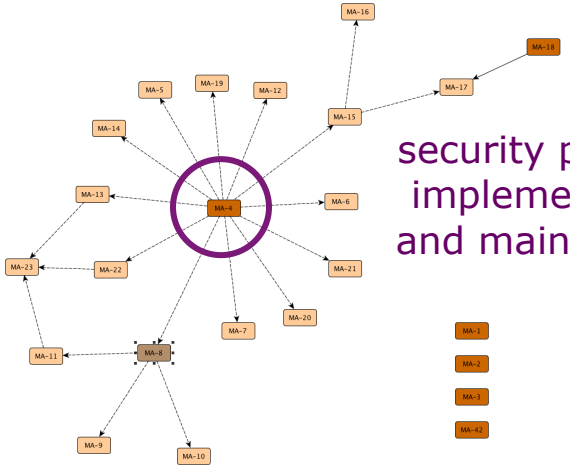
MD-16: may give notice by electronic mail to the individual

MD-20: may post the notice on the website of the business

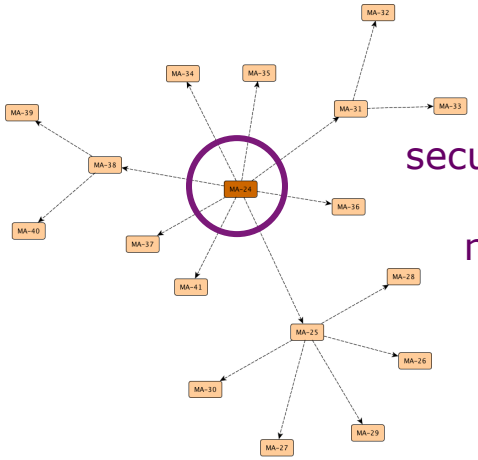
Legend: Surface Extension → Exception ----➤ Refines or Follows

Graph computed from Maryland Personal Information Protection Act

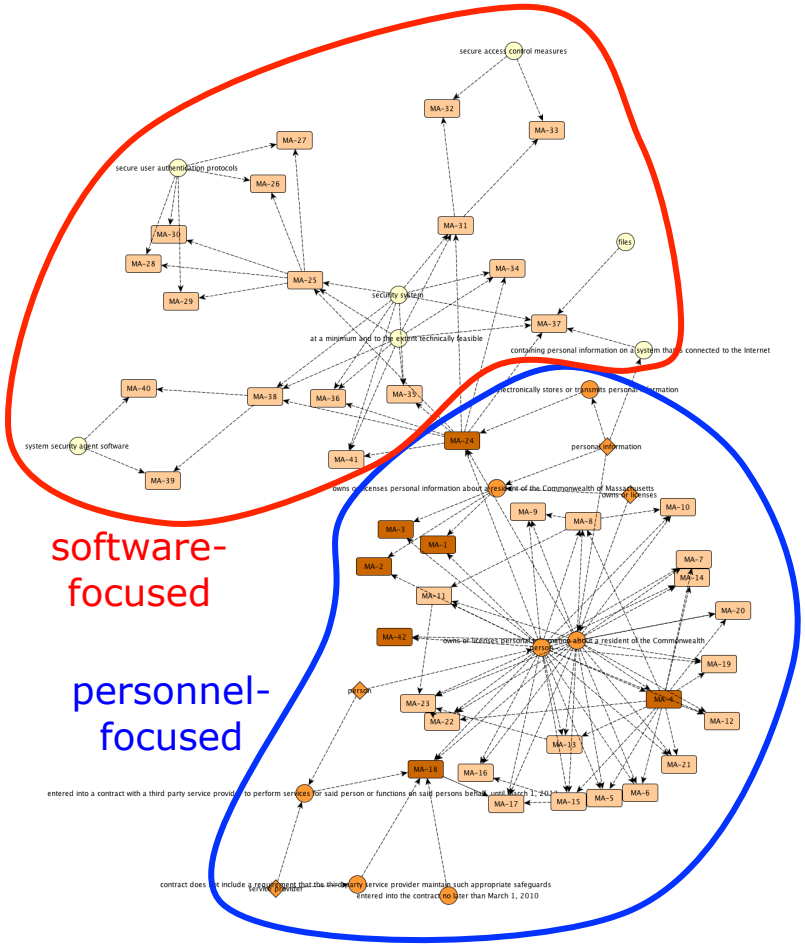
Surface Structure and Themes



security program implementation and maintenance



security program runtime monitoring



software-focused

personnel-focused

Contributions and Future Work

Contributions

- A systematic method for acquiring and formalizing requirements from regulations with traceability
- A reusable requirements model (standard upper ontology) validated in two domains
- Four new requirements prioritization methods:
  - Balancing rights with obligations
  - Stakeholder and product hierarchy
  - Requirements specialization
  - Requirements exception hierarchy
- A suite of tools that partially automate the method

Future Work Challenges

Requirements Analysis

- Transnational data privacy laws
- Collaborative legal requirements refinement

Requirements and System Specification

- Electronic rulemaking
- Trustworthy and compliant design

Thank you!

Feedback and Questions