A Method to Acquire Compliance Monitors from Regulations

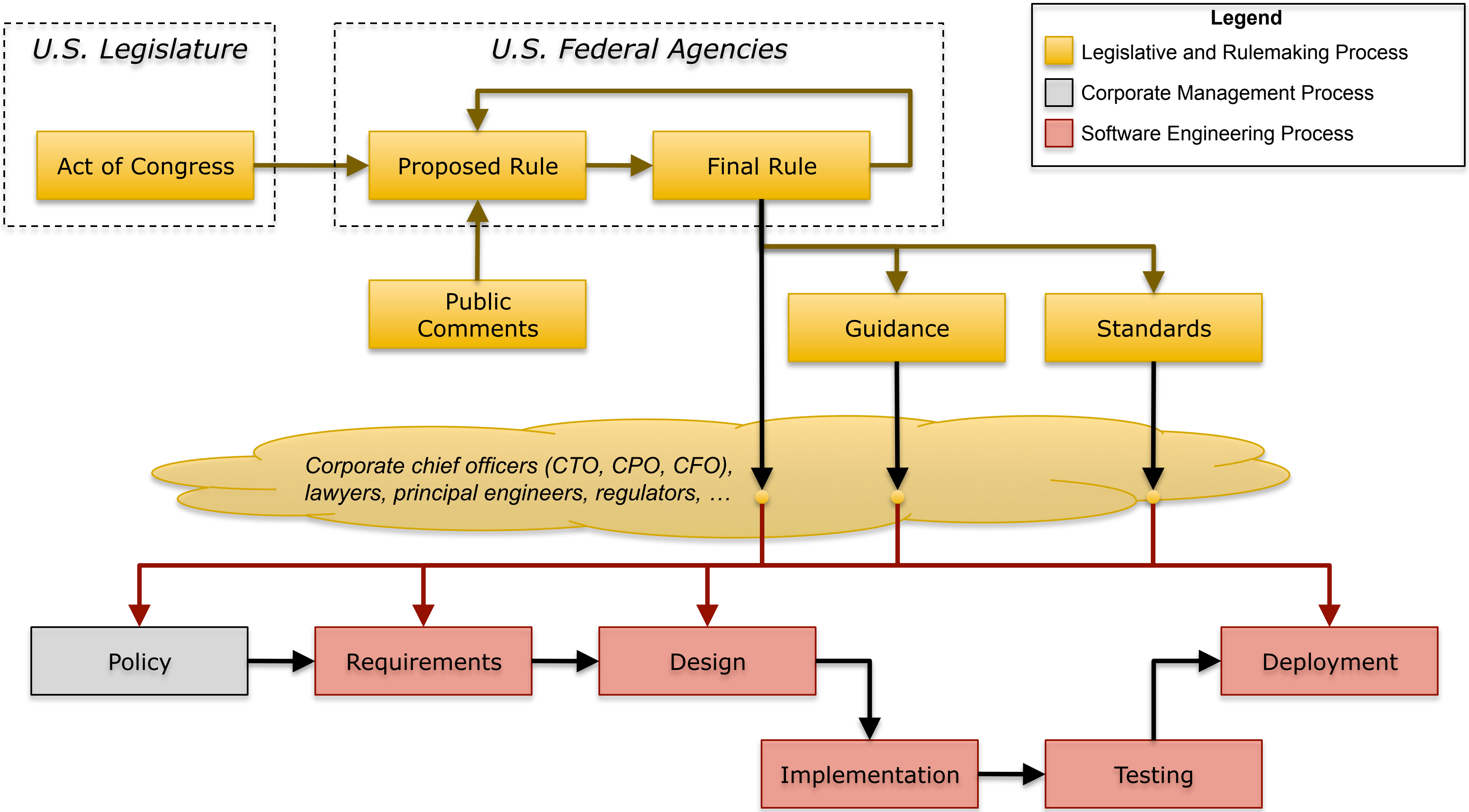
Travis D. Breaux

Institute for Software Research
Carnegie Mellon University
September 28, 2010

Presentation Overview

- Introduction
- Background and Motivation
- Related Work
- Methodology
- Summary and Findings

What do we mean by the law?



U.S. Legislature
U.S. Federal Agencies
Act of Congress
Proposed Rule
Final Rule
Public Comments
Guidance
Standards
Legend
🟨 Legislative and Rulemaking Process
⬜ Corporate Management Process
🟥 Software Engineering Process
Corporate chief officers (CTO, CPO, CFO), lawyers, principal engineers, regulators, …
Policy
Requirements
Design
Implementation
Testing
Deployment

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: Up to 6% consumer churn in healthcare; up to 5% in finance *[Ponemon, 2010]*

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.]

Related Work

- **AI:** Modeling Laws and Regulations

  Sherman (ICAIL'87); Sergot et al. (ICAIL'91); Kerrigan (ICAIL'03)

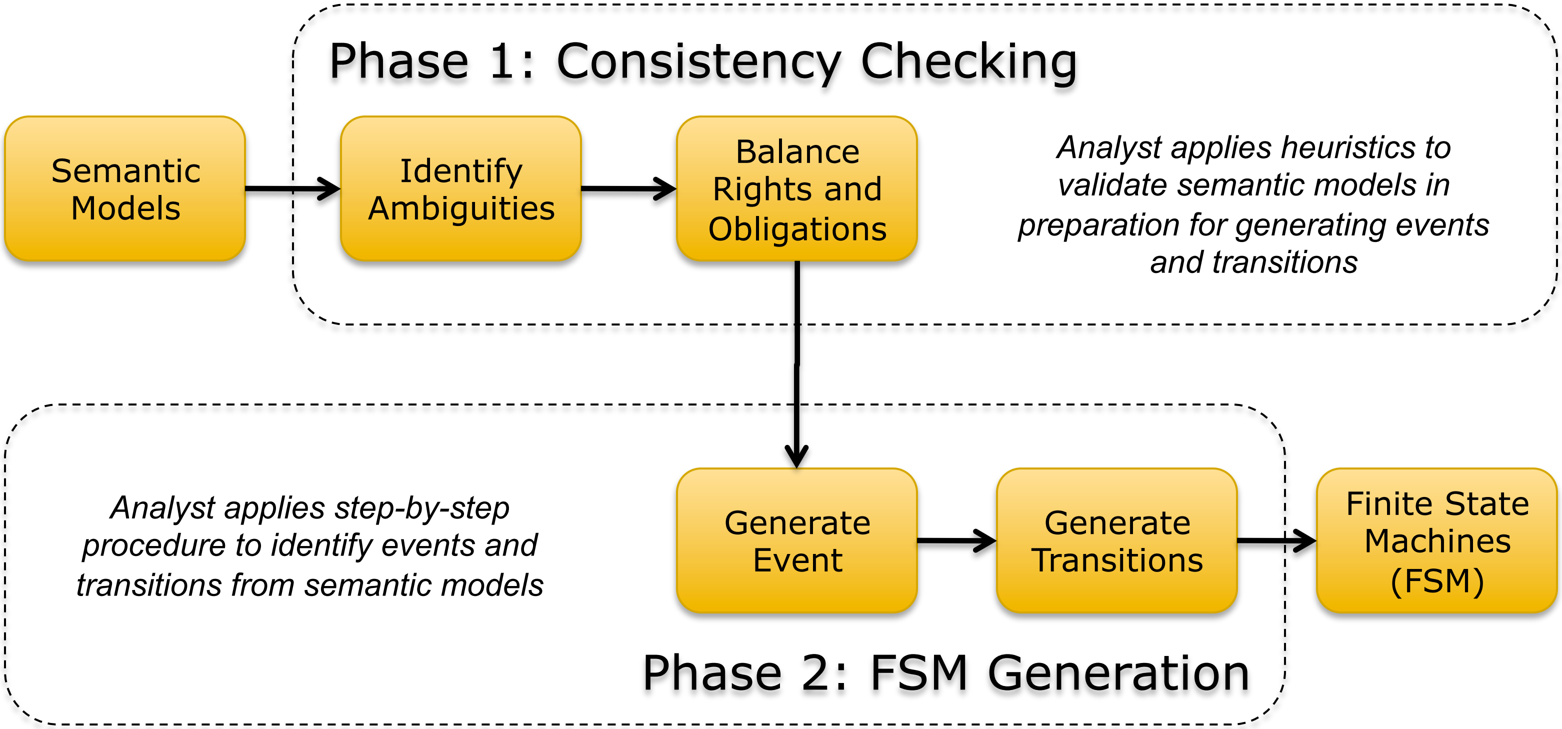
- **SE:** Model/Consistency Checking in Software

  Atlee, Gannon (SOCS'91); Bharadwaj, Heitmeyer (ASE'99); Chechik, Gannon (TSE'01); Heitmeyer, Jeffords, Labaw (TOSEM'96)

- **RE:** Runtime Requirements Monitoring

  Peters and Parnas (TSE'96); Fickas, Beauchamp, Mamy (ASE'02); Robinson (REJ'05)

Overview of the Method



Analyst applies heuristics to validate semantic models in preparation for generating events and transitions

Analyst applies step-by-step procedure to identify events and transitions from semantic models

What are Semantic Models?

Restricted Natural Language Statement (RNLS)

[IEEE RE 2005]

- The full scope of natural language is too complex!
- Each RNLS describes one activity with external references to other RNLSs.
- Rights and obligations are described by activities.

"The provider may share information to market services."

RNLS 1.1: The provider markets services.

RNLS 1.2: The provider may share information to (RNLS#1).

Semantic Model with Conditions

Stated Obligation

- ***$O_{4.10}$***: The covered entity (CE) must provide the individual access to PHI in the requested format.

Inferred Conditions

- ***C_1***: The individual requests to access the PHI in a format
- ***C_2***: The requested format is readily available

```
activity [ obligation ] {
    subject = CE
    action = provide
    object = access {
        subject = individual
        action = access
        object = PHI {
            format [ requested ]
        }
    }
    target = individual
}
```

Subject-Action-Object Triples

- We define the function T to map the set of legal requirements to triples consisting of a subject (S), action (A) and object (O)

  $T{:}L \rightarrow \langle S, A, O \rangle$

Example:

$T(O_{4.10}) = \langle \text{CE, provide, } X \rangle$

$T(X) = \langle \text{individual, access, PHI} \rangle$

```
activity [ obligation ] {
    subject = CE
    action = provide
    object = access {
        subject = individual
        action = access
        object = PHI {
            format [ requested ]
        }
    }
    target = individual
}
```

Phase 1

Consistency Checking

Identify Ambiguities

Missing Objects and Targets

- The covered entity must provide access.
  - ❑ Provide access to whom?
  - ❑ Provide access to what?

Missing Objects and Subjects

- … the requested access.
  - ❑ Who requested access?
  - ❑ Request access to what?
  - ❑ Request access from whom?

Balancing Rights and Obligations

[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

Phase 2

FSM Generation

Generating States and Transitions

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	$O_{6.3}$	$\neg E_1$	$NC_{6.3}$

```
activity [ obligation ] {
      subject = CE
      action = provide
      object = denial [ written ] {
                subject = CE
                action = deny
                object = request {
                        subject = Individual
                        action = request
                        object = amendment {
                                subject = CE
                                action = amend
                                object = PHI
                        }
                }
        }
        target = Individual
}
```

Visualizing Finite State Machines

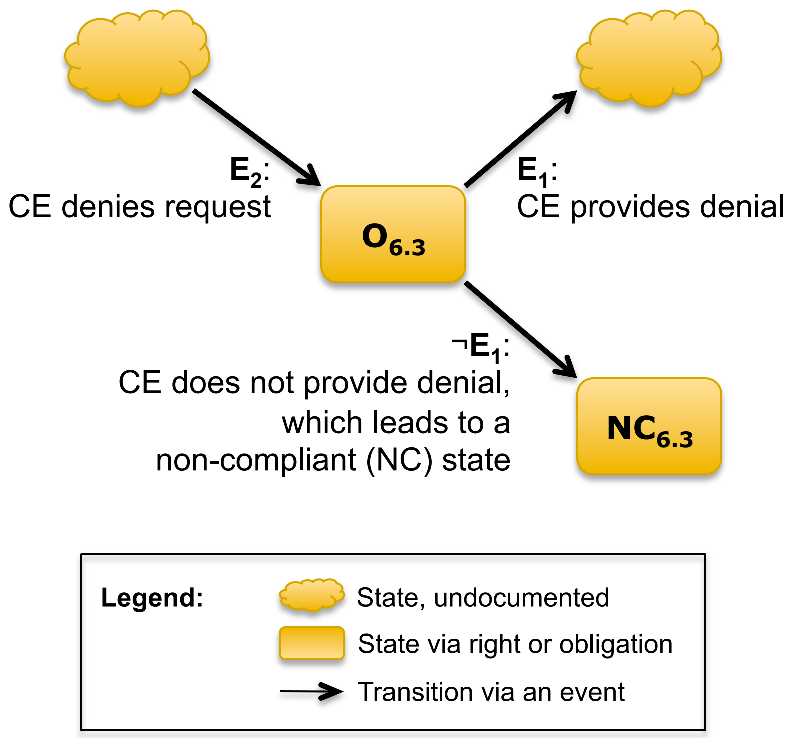
State-Event Table

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



E_2: CE denies request

E_1: CE provides denial

$O_{6.3}$

$\neg E_1$: CE does not provide denial, which leads to a non-compliant (NC) state

$NC_{6.3}$

Legend:

- State, undocumented
- State via right or obligation
- Transition via an event

Case Study

Analysis of HIPAA Privacy Rule §164.524

PART 164: SECURITY AND PRIVACY

Subpart E: Privacy of Individually Identifiable Health Information

Sec. 164.524 Access of individuals to protected health information.

(a) Standard: Access to protected health information--

(1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

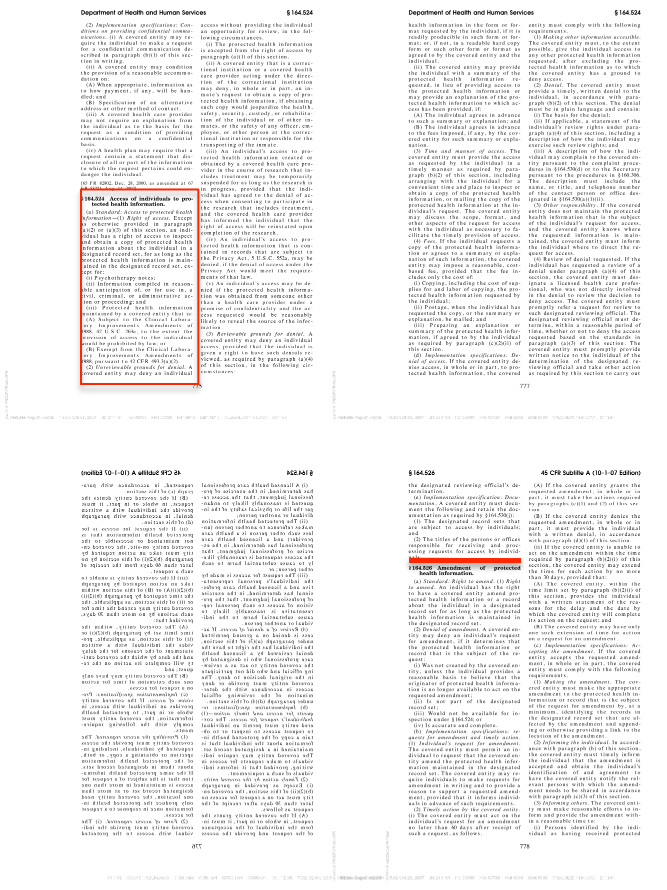
(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

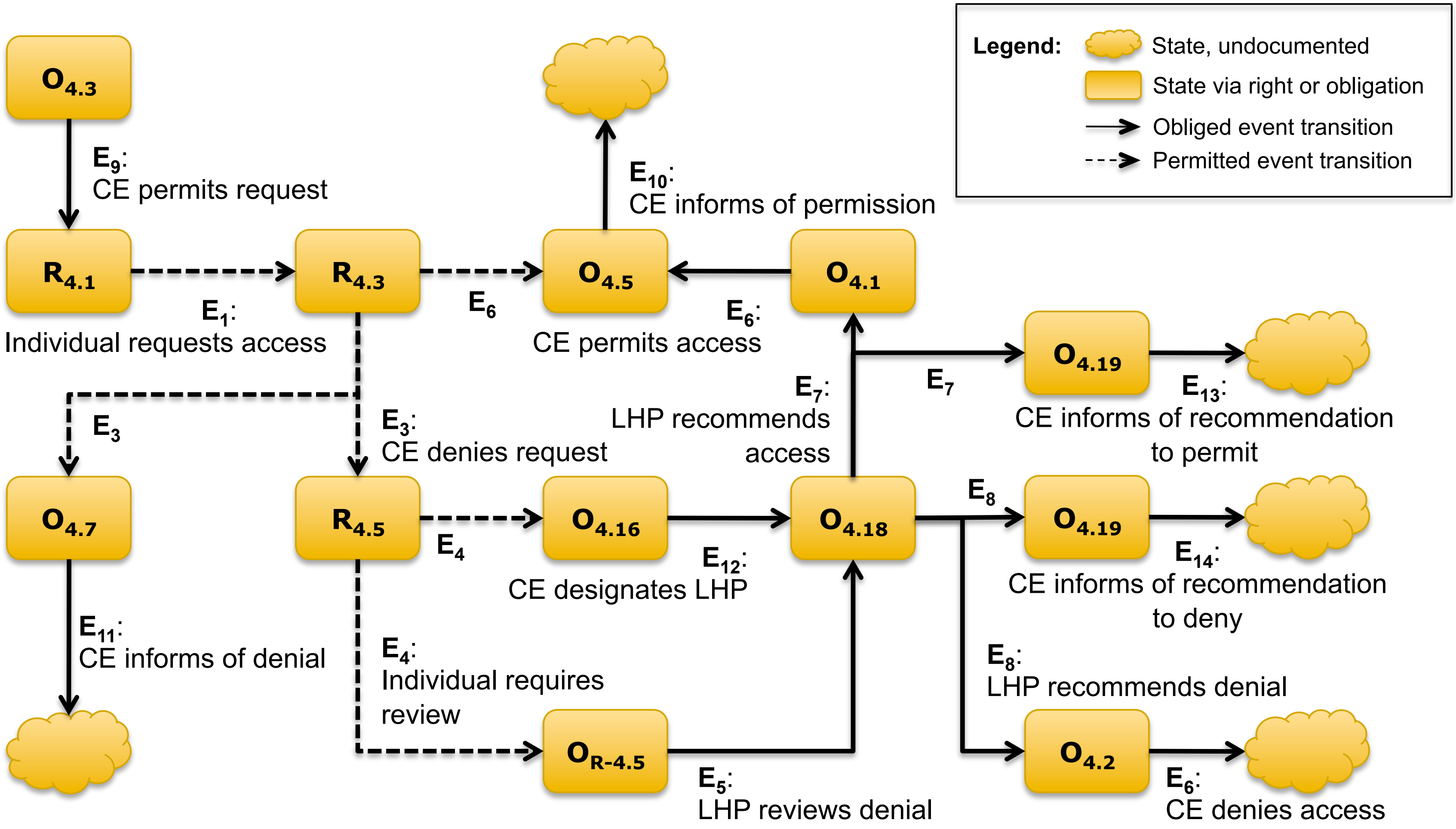
(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) Unreviewable grounds for denial. …



Combined Compliance Monitor

Acquired from HIPAA Privacy Rule §164.524



Legend:
State, undocumented
State via right or obligation
→ Obliged event transition
- - -> Permitted event transition

$O_{4.3}$

E_9:
CE permits request

$R_{4.1}$

E_1:
Individual requests access

$R_{4.3}$

E_6

$O_{4.5}$

E_{10}:
CE informs of permission

$O_{4.1}$

E_6:
CE permits access

E_7

$O_{4.19}$

E_{13}:
CE informs of recommendation to permit

E_3

E_3:
CE denies request

E_7:
LHP recommends access

$O_{4.7}$

$R_{4.5}$

E_4

$O_{4.16}$

$O_{4.18}$

E_8

$O_{4.19}$

E_{12}:
CE designates LHP

E_{14}:
CE informs of recommendation to deny

E_{11}:
CE informs of denial

E_4:
Individual requires review

E_8:
LHP recommends denial

$O_{R\text{-}4.5}$

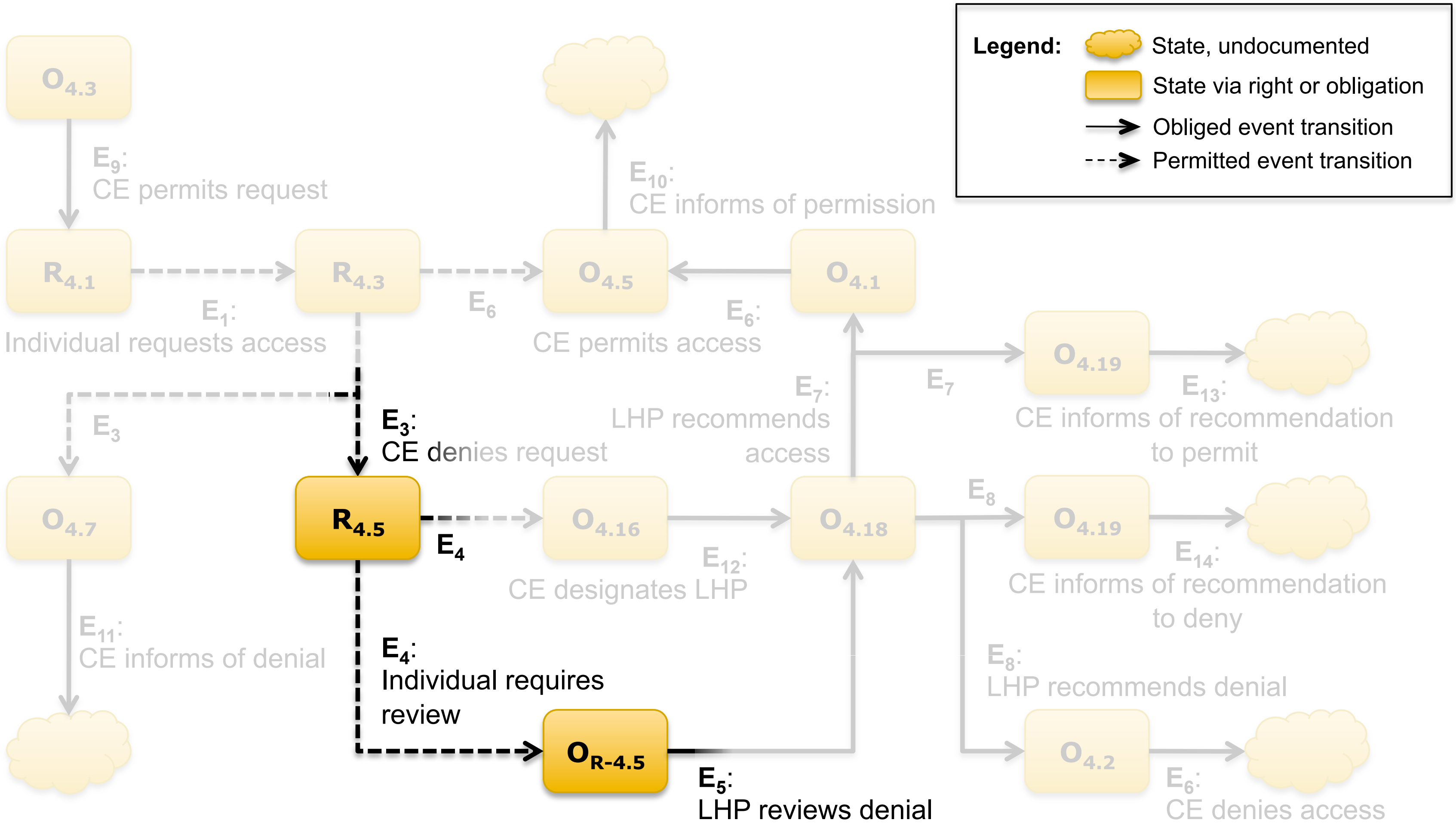
$O_{4.2}$

E_5:
LHP reviews denial

E_6:
CE denies access

Inferred States and Transitions

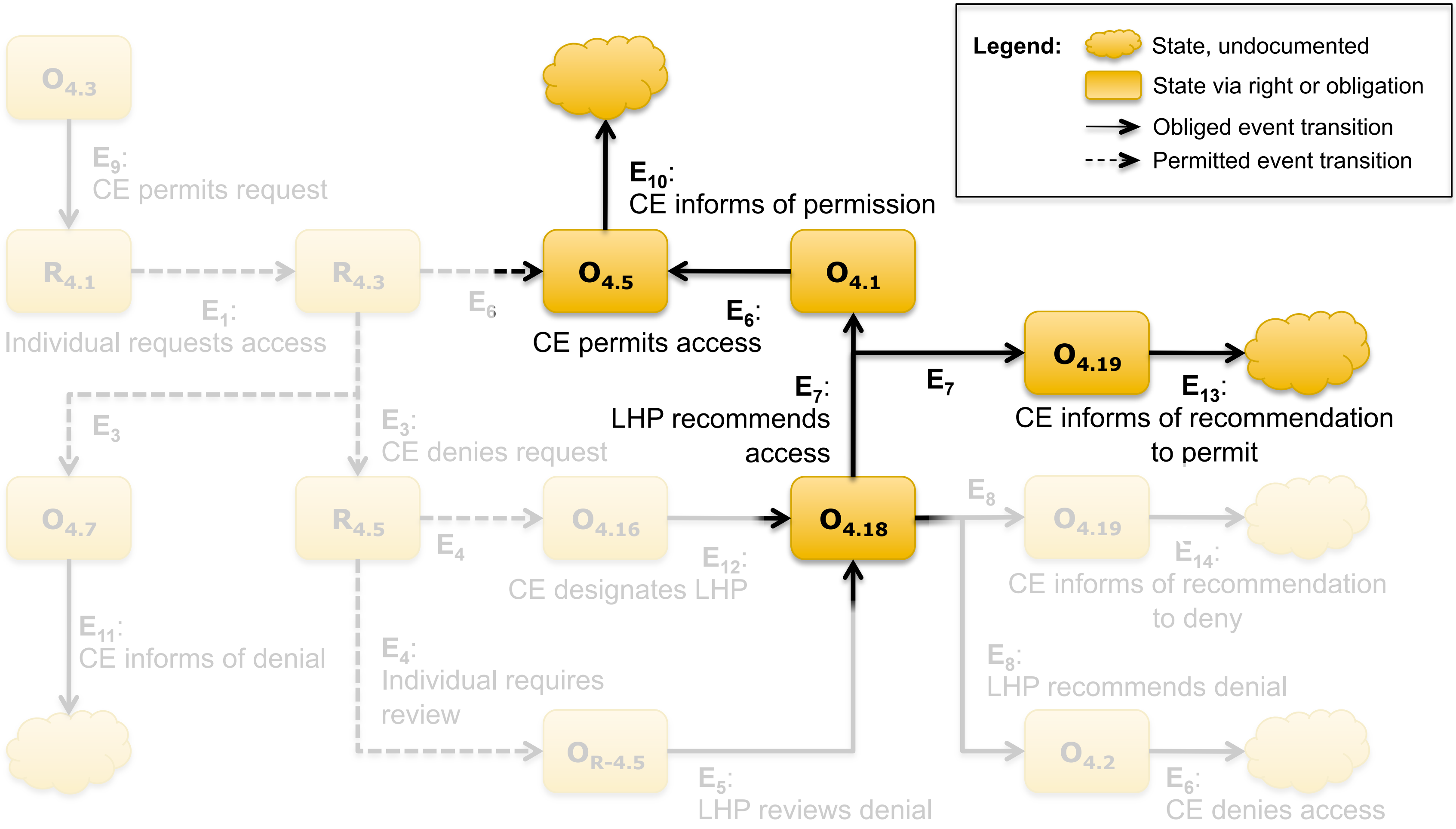
Acquired from HIPAA Privacy Rule §164.524



Legend:
State, undocumented
State via right or obligation
Obliged event transition
Permitted event transition
$O_{4.3}$
E_9: CE permits request
E_{10}: CE informs of permission
$R_{4.1}$
$R_{4.3}$
$O_{4.5}$
$O_{4.1}$
E_1: Individual requests access
E_6
E_6: CE permits access
$O_{4.19}$
E_7
E_{13}: CE informs of recommendation to permit
E_3
E_3: CE denies request
E_7: LHP recommends access
$O_{4.7}$
$R_{4.5}$
E_4
$O_{4.16}$
$O_{4.18}$
E_8
$O_{4.19}$
E_{12}: CE designates LHP
E_{14}: CE informs of recommendation to deny
E_{11}: CE informs of denial
E_4: Individual requires review
E_8: LHP recommends denial
$O_{R-4.5}$
$O_{4.2}$
E_5: LHP reviews denial
E_6: CE denies access

Identifying Duplicitous Events

Acquired from HIPAA Privacy Rule §164.524



Legend: State, undocumented

State via right or obligation

Obligated event transition

Permitted event transition

$O_{4.3}$

E_9: CE permits request

$R_{4.1}$

E_1: Individual requests access

$R_{4.3}$

E_6

$O_{4.5}$

E_{10}: CE informs of permission

$O_{4.1}$

E_6: CE permits access

E_7

$O_{4.19}$

E_{13}: CE informs of recommendation to permit

E_7: LHP recommends access

E_3

E_3: CE denies request

$O_{4.7}$

$R_{4.5}$

E_4

$O_{4.16}$

E_{12}: CE designates LHP

$O_{4.18}$

E_8

$O_{4.19}$

E_{14}: CE informs of recommendation to deny

E_{11}: CE informs of denial

E_4: Individual requires review

E_8: LHP recommends denial

$O_{R-4.5}$

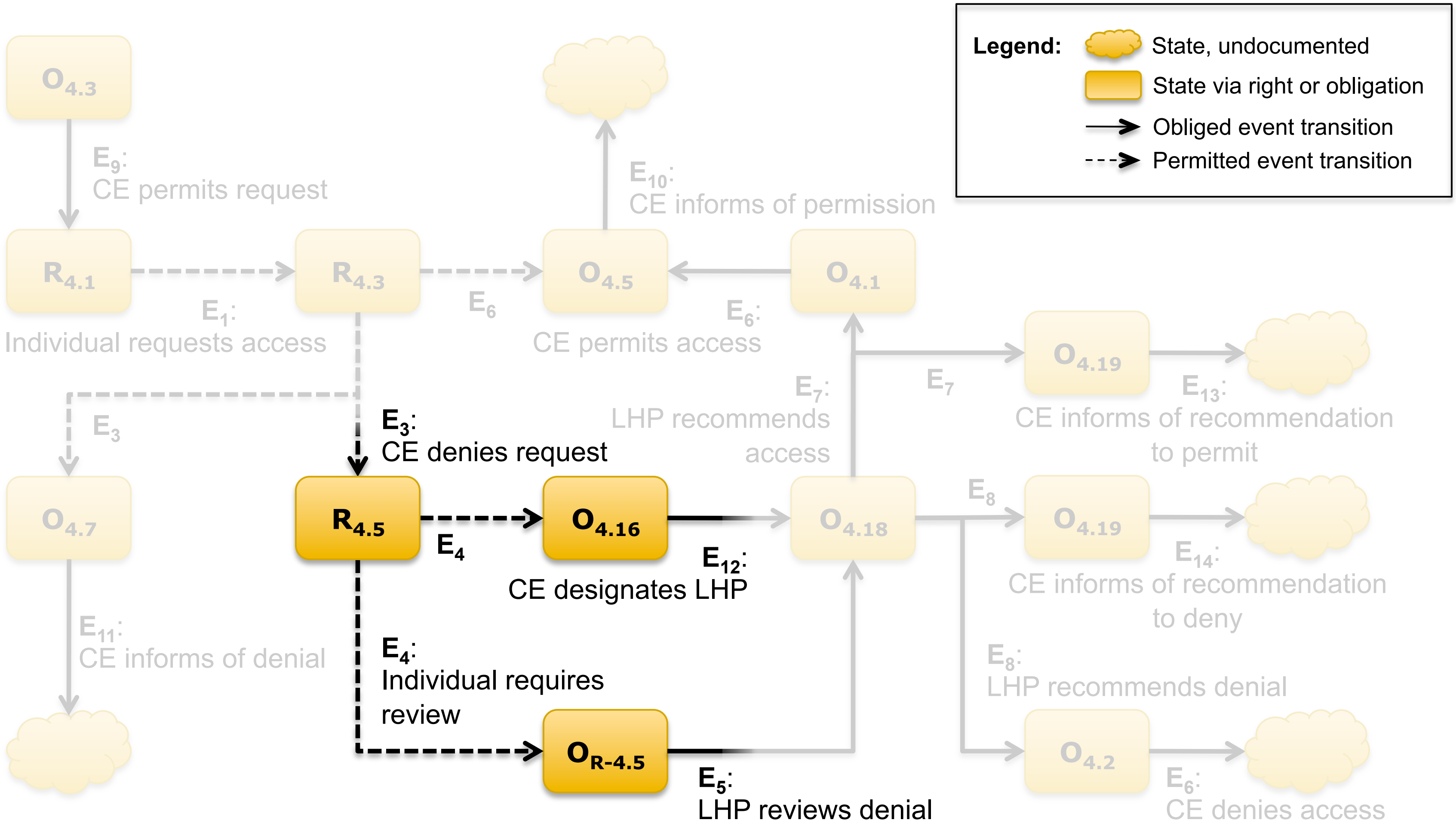
E_5: LHP reviews denial

$O_{4.2}$

E_6: CE denies access

Identifying Implied Pre-Conditions

Acquired from HIPAA Privacy Rule §164.524



Legend:

- ☁ State, undocumented
- ▭ State via right or obligation
- → Obliged event transition
- ⇢ Permitted event transition

$O_{4.3}$

E_9: CE permits request

E_{10}: CE informs of permission

$R_{4.1}$

$R_{4.3}$

$O_{4.5}$

$O_{4.1}$

E_1: Individual requests access

E_6

E_6: CE permits access

E_7: LHP recommends access

E_7

$O_{4.19}$

E_{13}: CE informs of recommendation to permit

E_3

E_3: CE denies request

$O_{4.7}$

$R_{4.5}$

E_4

$O_{4.16}$

E_{12}: CE designates LHP

$O_{4.18}$

E_8

$O_{4.19}$

E_{14}: CE informs of recommendation to deny

E_{11}: CE informs of denial

E_4: Individual requires review

E_8: LHP recommends denial

$O_{R\text{-}4.5}$

E_5: LHP reviews denial

$O_{4.2}$

E_6: CE denies access

Issues and Future Work

- We claim that some form of computable model can be provided to companies seeking to comply with some laws
- For this purpose, our method aids in the identification of:
  - Inferred states
  - Duplicitous events
  - Implied pre-conditions
- For future work, what notation should be used to express the models in a way to enable runtime monitoring?
  - Business process models
  - Architecture description languages