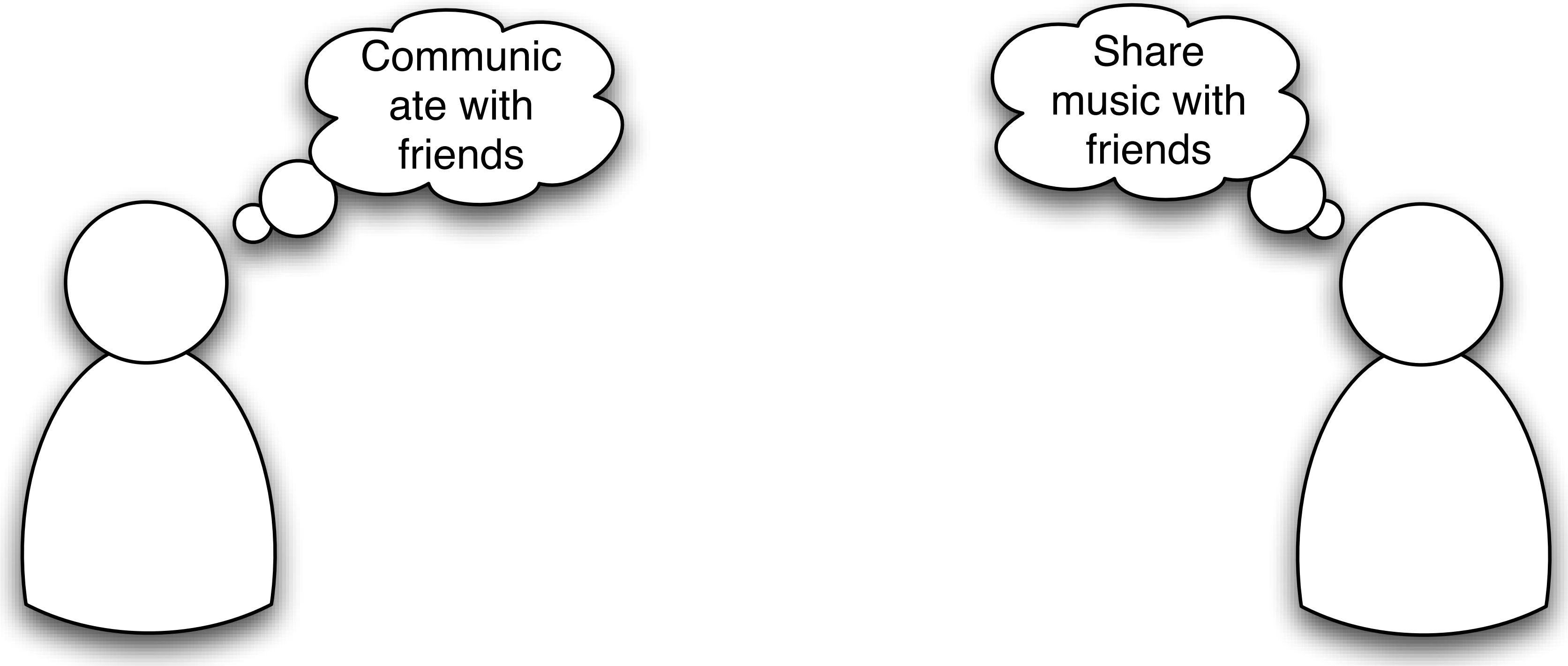
Requirements compliance engineering: exploring legal alternatives

Alberto Siena

- Motivation
  - Problem
  - Intuition for a solution
- The language for exploring norms
  - A bit of formalism
- Examples of use

The role of law in RE

$$S, K \vdash R$$



The role of law in RE

- Law is part of the environment, which the STS operates in
- Laws affect requirements but are not stakeholder requirements
  - Point-of-view mismatch
    (actor's interests vs. legislator's interests)
  - Abstraction gap
    (domain level vs. "cross-domain" level)

The complexity problem

- Law states norms together with the **conditions** for their **applicability**
- Italian Data Protection Code
  - **“If data processing is carried out with the help of electronic means**, then the data subject shall have the right to be informed
  - The rights may not be exercised by making a request to the data controller or processor **if the personal data are processed**
    - pursuant to the provisions of decree-law no. blah blah
    - by a public body other than a profit-seeking public body…
  - Exercise of the rights may be permitted **with regard to data of nonobjective character on condition that** it does not concern…

Why a requirements problem?

- Not all systems-to-be are subject to the same norms
  - they have different purposes
  - **the same purpose can be achieved in different ways**
- By choosing the requirements that the system-to-be should satisfy, the requirements engineer chooses the **conditions** that the system-to-be will satisfy, and therefore also the norms that the system-to-be **should comply to**

Objectives

- *Include preconditions and postconditions* of legal norms and their relationships into early *representations of the requirements* problem and solution space
- Use this information to **evaluate the applicability and satisfiability of norms for given sets of requirements**, and thereby the **compliance** of these requirements.
- Eventually through automatic reasoning

Norm models

- *$\mathscr{L}$ = {N, S, R}*
- *Norm := Tuple (T, R, A, P)*
  - *T = Norm Type*
    - Duty: Pre → $\square$Con
    - Right: Pre → $\Diamond$Con
  - *R = Role*
  - *A = Applicability condition (precedent)*
  - *P = Satisfaction condition (consequent)*

Compliance

- A norm **applies** to an actor if and only if the actor *finds herself in a situation that satisfies the precondition of the norm*
- A norm is **satisfied** by an actor if and only if the actor *find herself in a situation that satisfies the provision of the norm*
- The actor **complies** with a norm if *that norm applies to that actor* ***and*** *the actor satisfies that norm*

Situation

- Partial state of the world
- Represents conditions
- Expressed through a proposition
  - Logical formula
  - Natural language
- Can be evaluated as as True or False (or Unknown)
- E.g.: “The gate is open”, “the light is blinking”

Relations

- Application relations
  - Relate situations to norm, and norms to other norms
  - Trigger or prevent norms applicability
- Satisfaction relation
  - Relate situations to norm, and norms to other norms
  - Trigger or prevent norms satisfaction

	If source is	**Target is**
Activate	Sat	App
Block	Sat	Not App
Satisfy	Sat	Sat
Break	Sat	Not Sat
Endorse	App, Sat	App
Derogate	App, Sat	Not App

Example

- It is forbidden to stop the car on a motorway. In case of a car failure is permitted to stop the car on the motorway, provided that blinking lights are switched on. In case of heavy snow, it is mandatory to stop the car on the motorway and install snow chain on the car.

Google driverless car

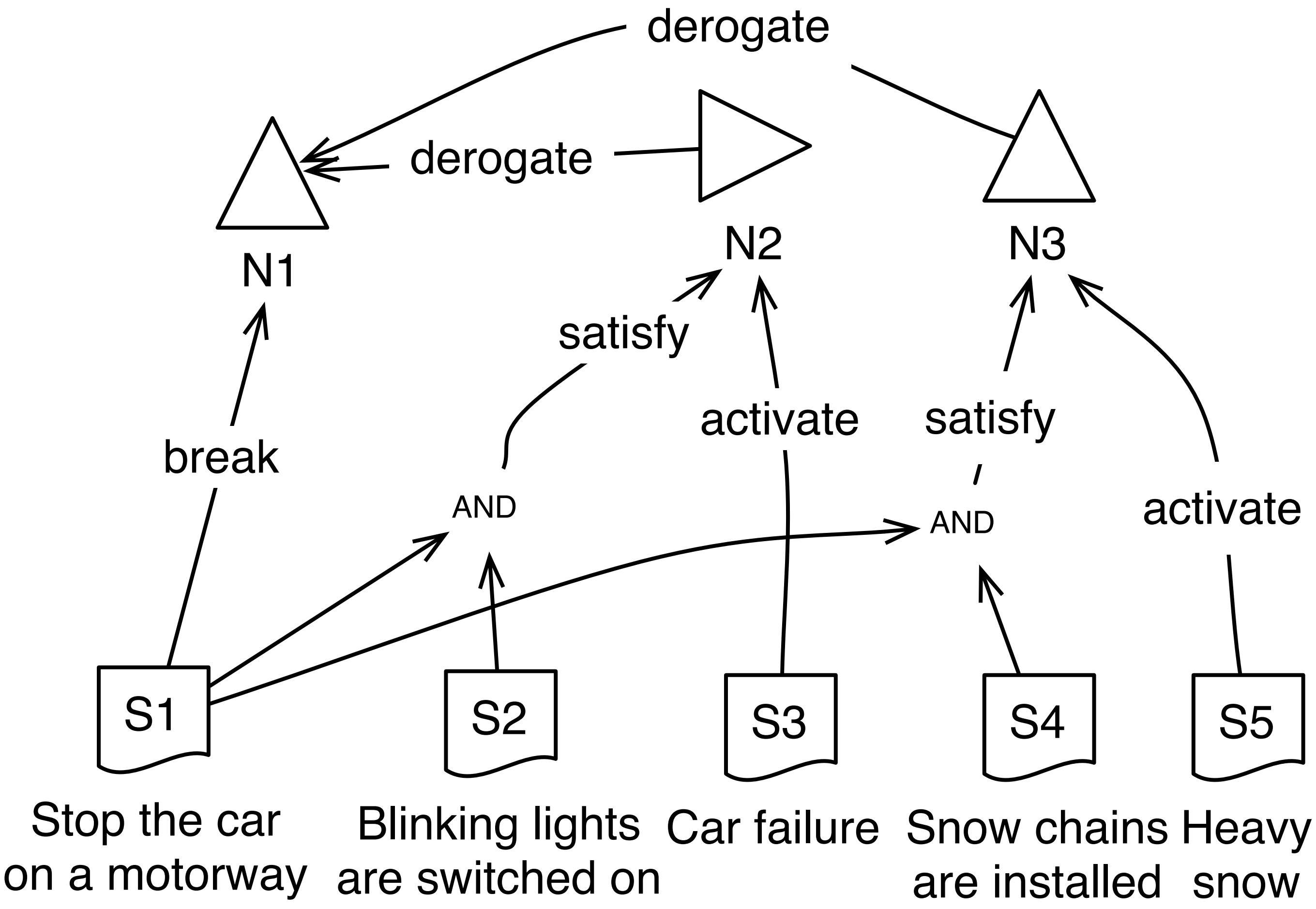
Example

- It is forbidden to stop the car on a motorway. In case of a car failure is permitted to stop the car on the motorway, provided that blinking lights are switched on. In case of heavy snow, it is mandatory to stop the car on the motorway and install snow chain on the car.
- S1 = “stop the car on a motorway”
- S2 = “there is a car failure”
- S3 = “blinking lights are switched on”
- S4 = “snow chains are installed”
- S5 = “there is snow”

Example

- It is forbidden to stop the car on a motorway. In case of a car failure is permitted to stop the car on the motorway, provided that blinking lights are switched on. In case of heavy snow, it is mandatory to stop the car on the motorway and install snow chain on the car.
- N1 = Prohibition
- N2 = Permission
- N3 = Obligation

Example


derogate
derogate
N1
N2
N3
break
satisfy
activate
satisfy
activate
AND
AND
S1
S2
S3
S4
S5
Stop the car on a motorway
Blinking lights are switched on
Car failure
Snow chains are installed
Heavy snow

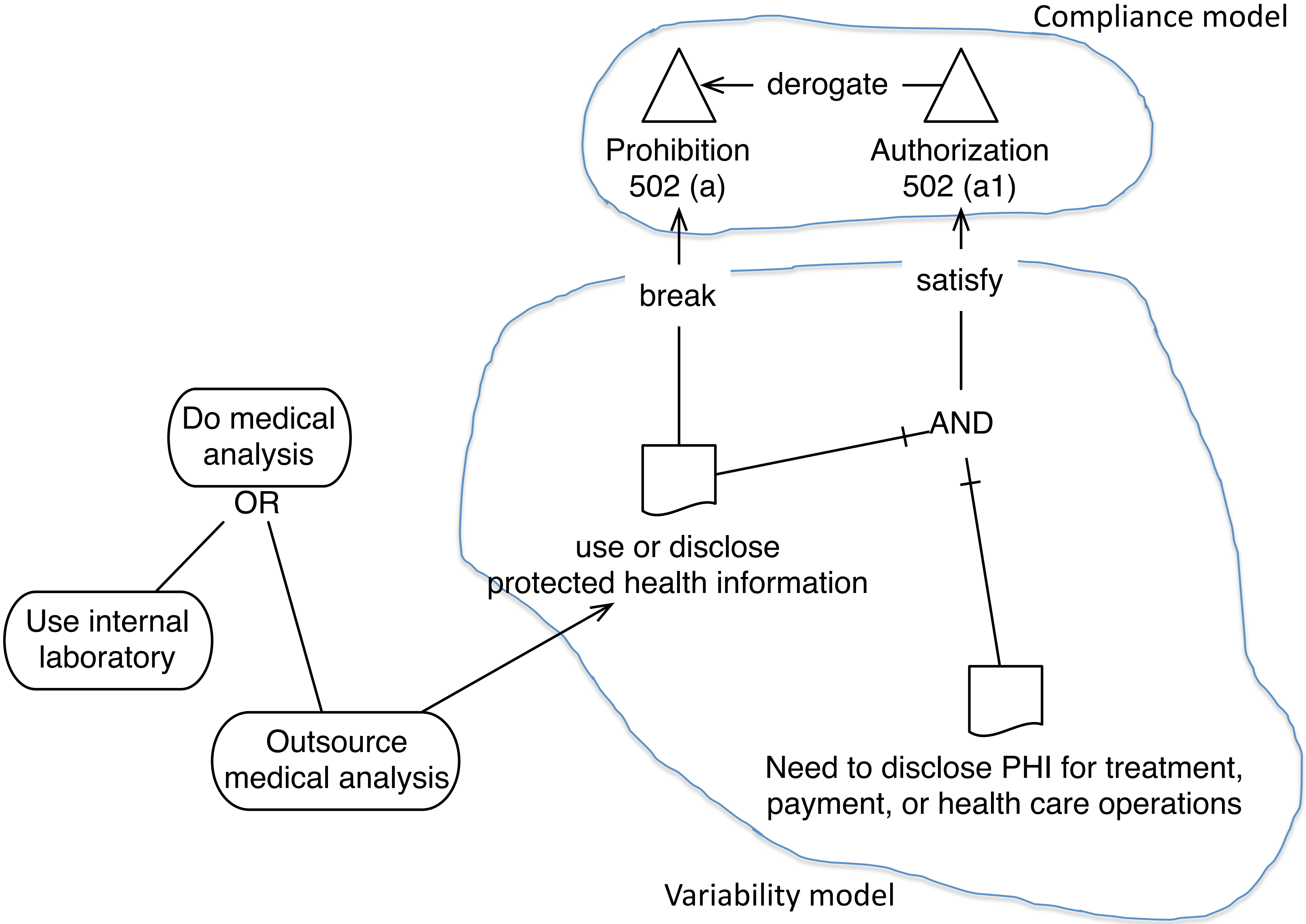
Exploring alternatives

- U.S. HIPAA 45CFR164.502
  - (a) A covered entity may not use or disclose protected health information, except as permitted or required by this subpart.
  - (a1) A covered entity is permitted protected health information [...] (payment, or health care operation compliance with Sec. 164.506;
  - (a2) A covered entity is required to disclose protected health information [...] (ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

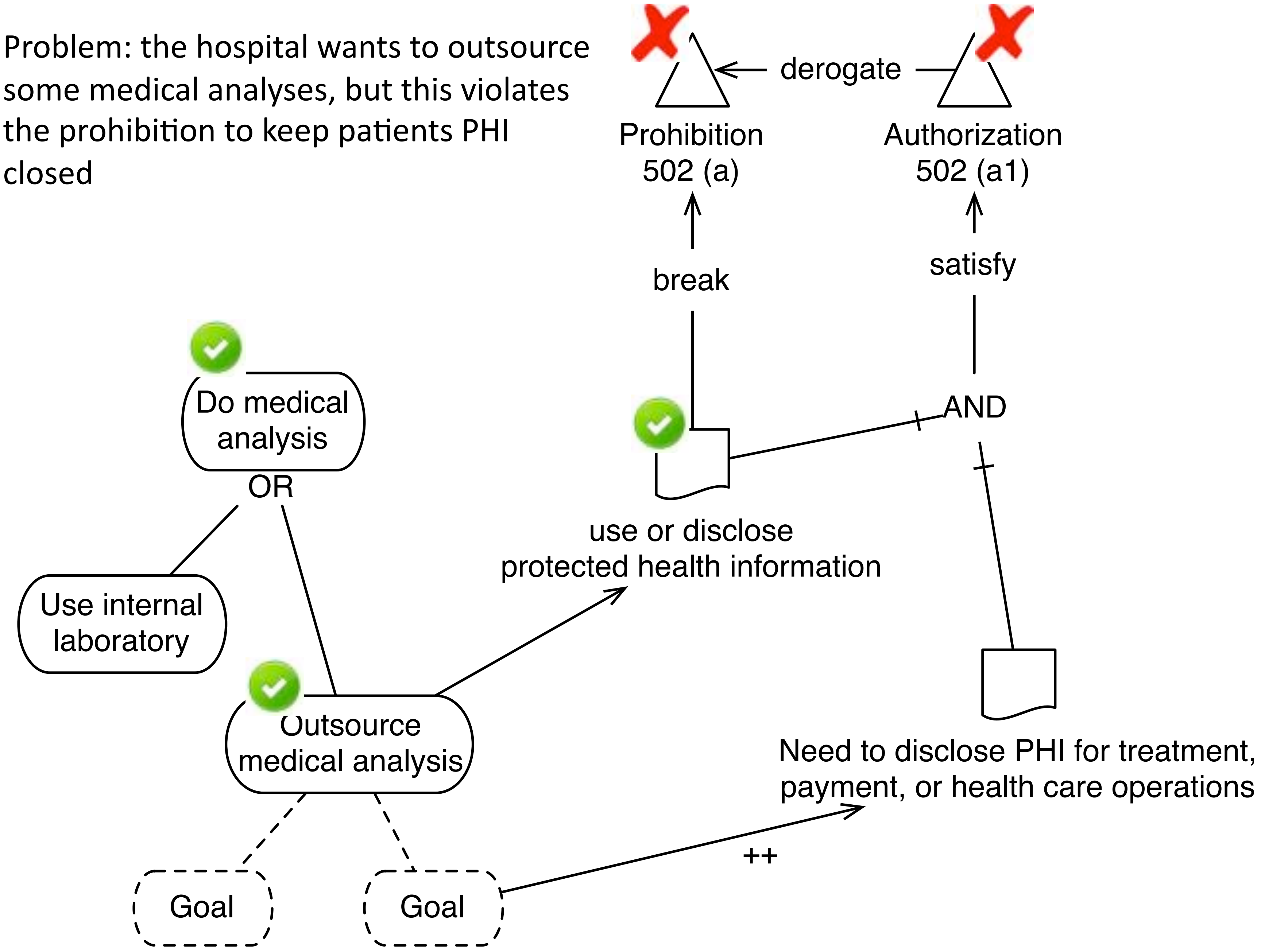
Same actor
Same action
Different norm types
Different conditions
Derogations

Questions

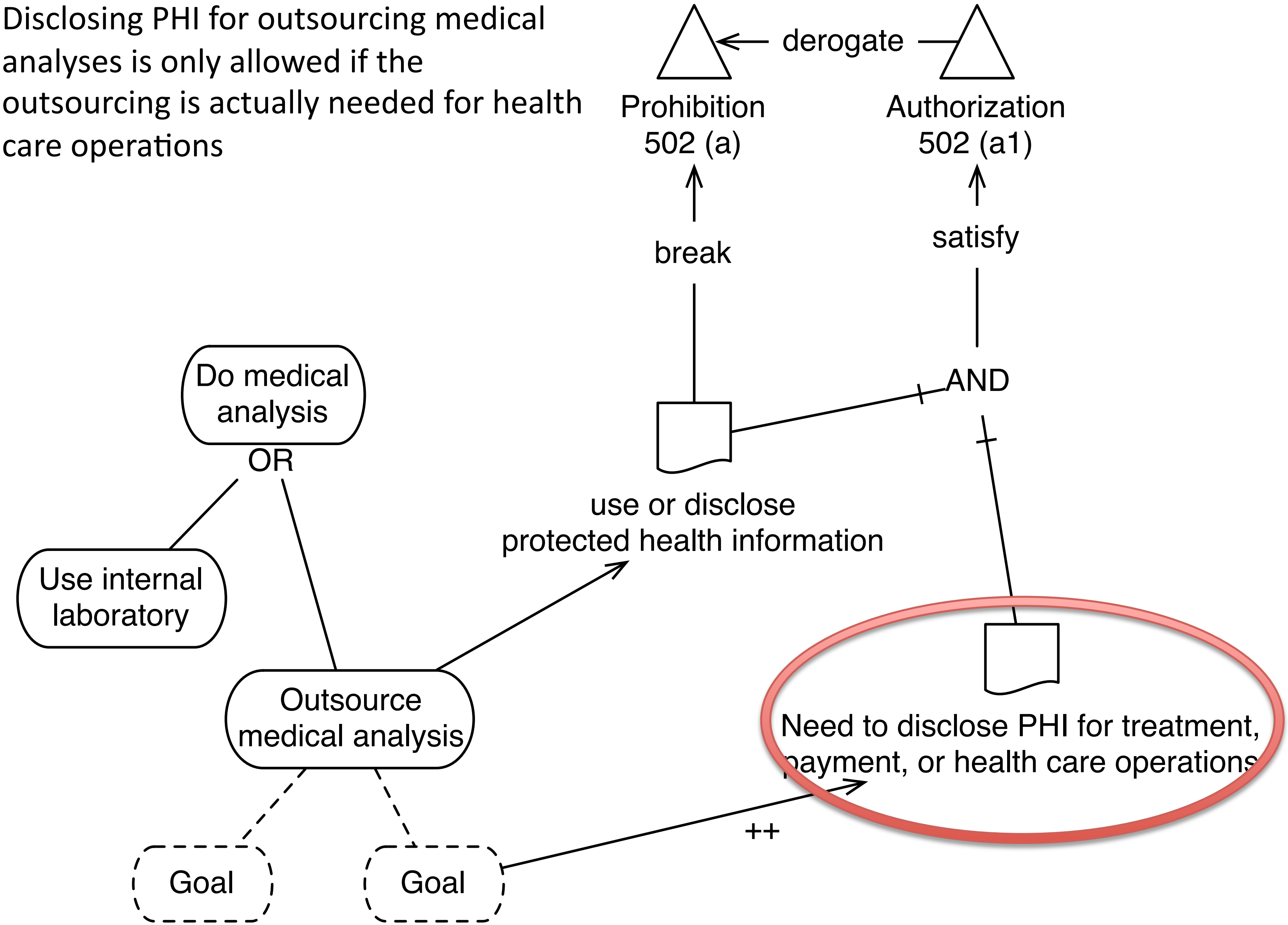
- **Given** a law, containing **a set of norms** articulated though conditions, exceptions and so on, **which of them apply to a given requirements model**?
  - Bottom-up analysis
- **Given a desired top-level requirement, how to select a compliant way to achieve it**, that is, a way which satisfies law applicable to it?
  - Top-down analysis
- Link goals to situations


Compliance model
derogate
Prohibition
502 (a)
Authorization
502 (a1)
break
satisfy
AND
Do medical analysis
OR
Use internal laboratory
Outsource medical analysis
use or disclose protected health information
Need to disclose PHI for treatment, payment, or health care operations
Variability model

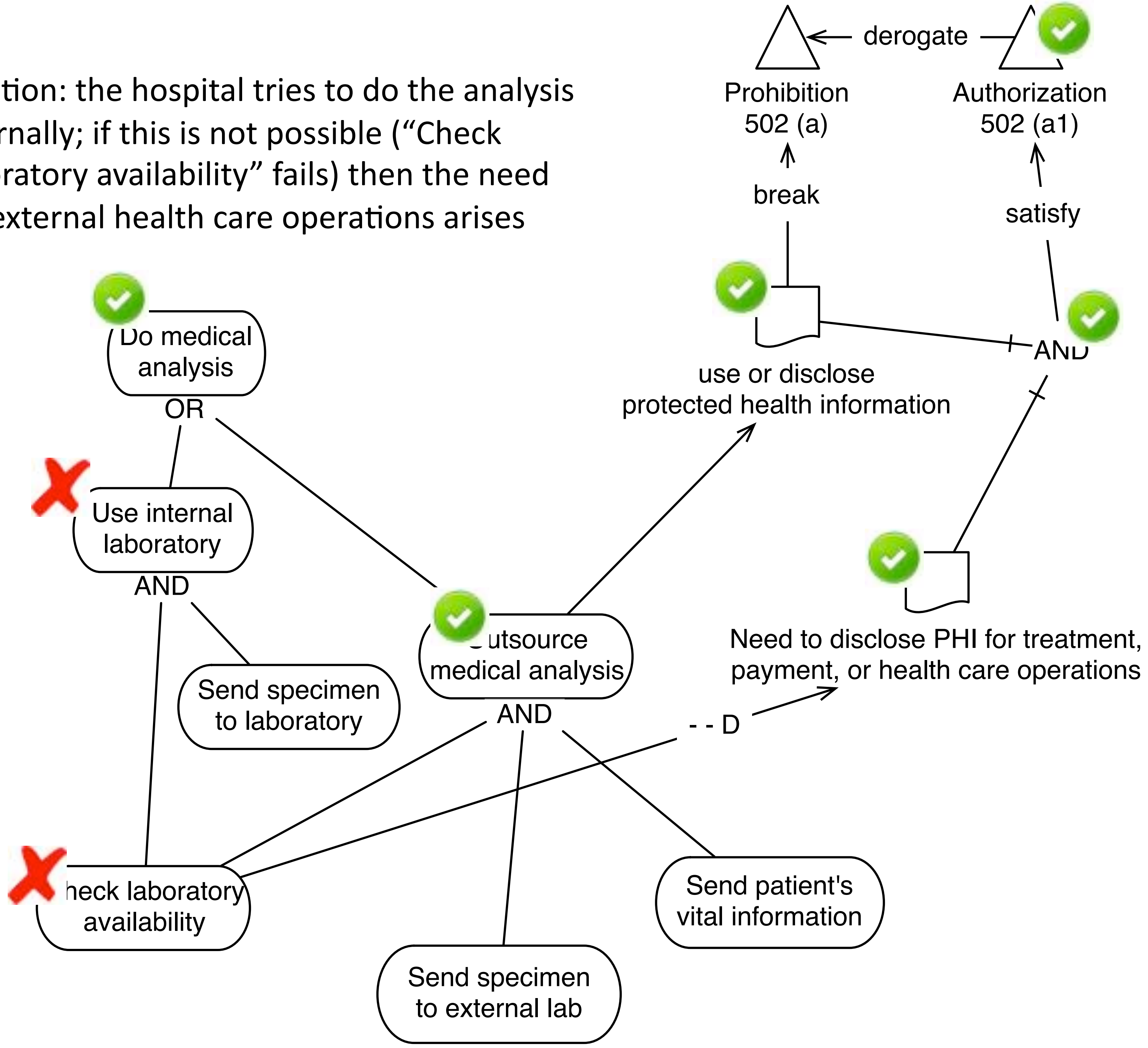
Problem: the hospital wants to outsource some medical analyses, but this violates the prohibition to keep patients PHI closed


derogate
Prohibition 502 (a)
Authorization 502 (a1)
break
satisfy
Do medical analysis
OR
AND
use or disclose protected health information
Use internal laboratory
Outsource medical analysis
Need to disclose PHI for treatment, payment, or health care operations
++
Goal
Goal

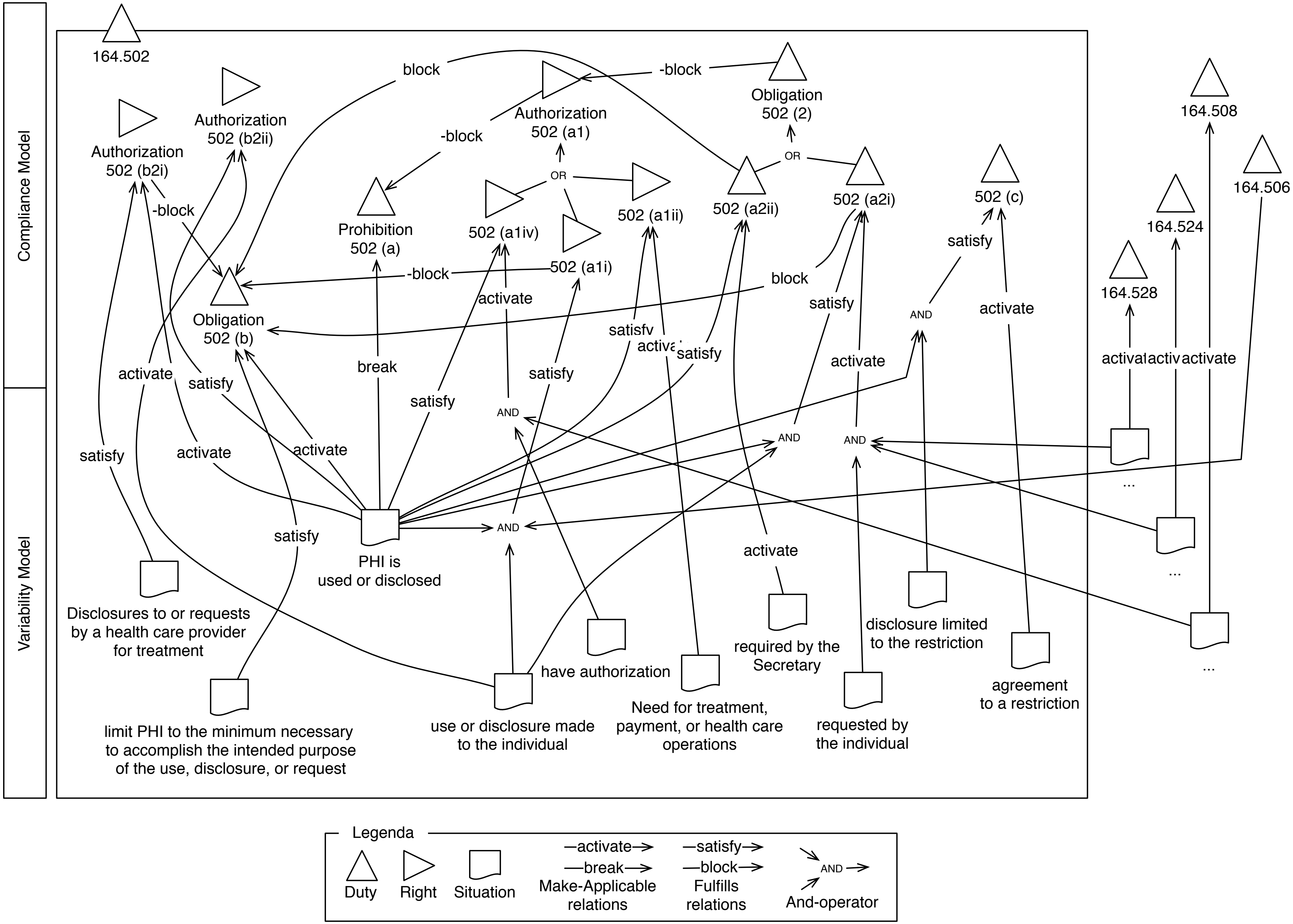
Disclosing PHI for outsourcing medical analyses is only allowed if the outsourcing is actually needed for health care operations


derogate
Prohibition 502 (a)
Authorization 502 (a1)
break
satisfy
AND
Do medical analysis
OR
use or disclose protected health information
Use internal laboratory
Outsource medical analysis
Need to disclose PHI for treatment, payment, or health care operations
++
Goal
Goal

Solution: the hospital tries to do the analysis internally; if this is not possible ("Check laboratory availability" fails) then the need for external health care operations arises



derogate
Prohibition 502 (a)
Authorization 502 (a1)
break
satisfy
AND
use or disclose protected health information
Do medical analysis
OR
Use internal laboratory
AND
Outsource medical analysis
AND
Need to disclose PHI for treatment, payment, or health care operations
- - D
Send specimen to laboratory
heck laboratory availability
Send patient's vital information
Send specimen to external lab



Compliance Model
Variability Model
164.502
Authorization
502 (b2i)
Authorization
502 (b2ii)
block
-block
Authorization
502 (a1)
-block
Obligation
502 (2)
OR
OR
Prohibition
502 (a)
502 (a1iv)
502 (a1i)
502 (a1ii)
502 (a2ii)
502 (a2i)
502 (c)
-block
-block
Obligation
502 (b)
block
satisfy
activate
satisfy
activate
satisfy
activate
break
satisfy
activate
satisfy
satisfy
activa
satisfy
satisfy
activate
activate
AND
satisfy
activate
AND
AND
AND
AND
164.508
164.524
164.506
164.528
activa
activ
activate
...
...
...
PHI is
used or disclosed
Disclosures to or requests
by a health care provider
for treatment
limit PHI to the minimum necessary
to accomplish the intended purpose
of the use, disclosure, or request
use or disclosure made
to the individual
have authorization
Need for treatment,
payment, or health care
operations
required by the
Secretary
requested by
the individual
disclosure limited
to the restriction
agreement
to a restriction
Legenda
Duty
Right
Situation
—activate→
—break→
Make-Applicable
relations
—satisfy→
—block→
Fulfills
relations
AND
And-operator

THANK YOU