An Access Control Language for a General Provenance Model

QUN NI[1], SHOUHUAI XU[2], ELISA BERTINO[1], RAVI SANDHU[2], AND WEILI HAN[3]

[1]PURDUE UNIVERSITY USA

[2]UT SAN ANTONIO USA

[3]FUDAN UNIVERSITY CHINA

PRESENTED BY

GABRIEL GHINITA

What is Provenance

- Healthcare
  - who provides the treatment based on what observation
  - who carries on the operation, and when
- Scientific Computing
  - the support of the protein functionality predication
  - the algorithm used to fold the protein
- Forensic
  - the source of evidence

Why Need An Access Control on Provenance

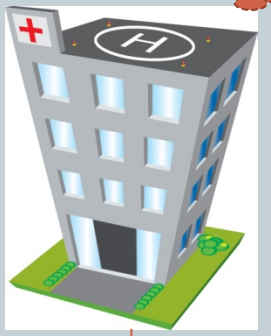
- Provenance is sensitive
  - The patient privacy, e.g. health situation, treatment, etc.
  - The proprietary algorithm used to predicate protein functionalities
  - The security of the source of evidences
- Therefore, we need a mechanism to control the access on provenance.
- However, provenance access control results in some new research challenges

Motivati

HIPAA:
Purpose based

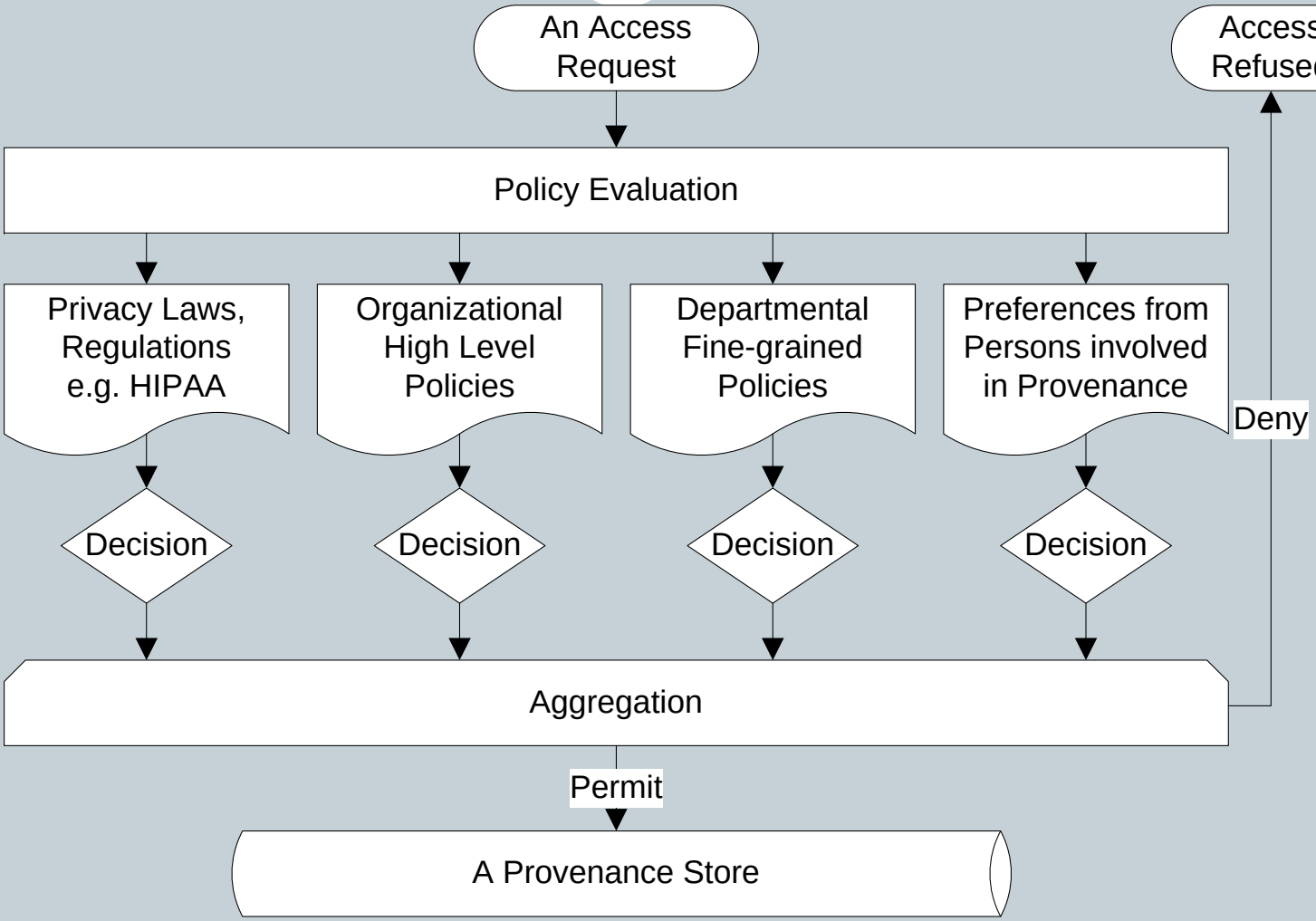
Hospital: Only
by employees
on duty

Department: at
working time, or
specific machine



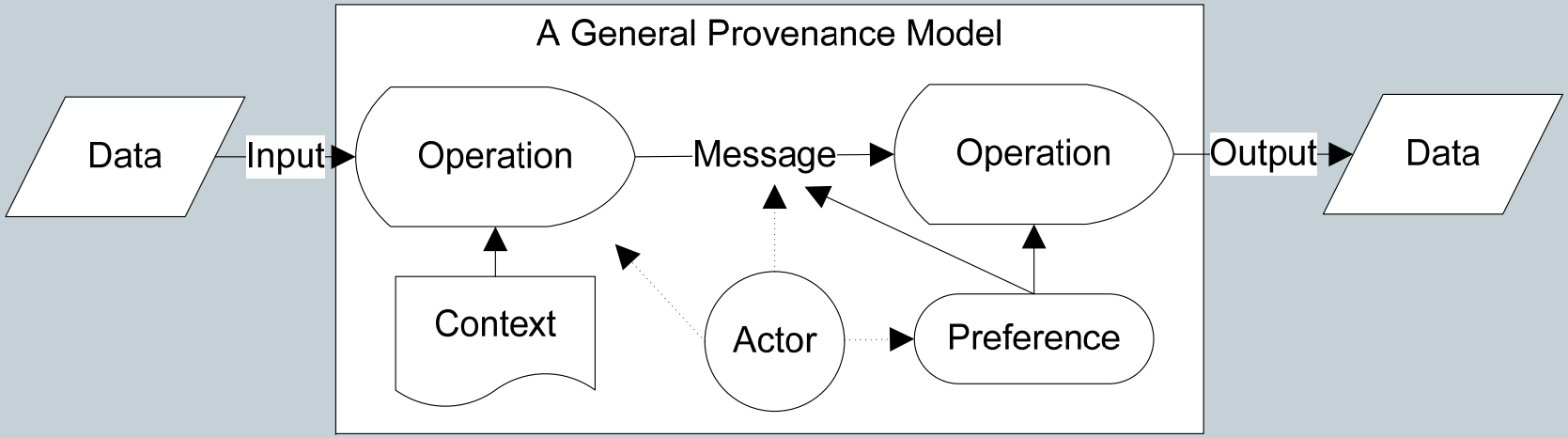
Patient: only
for research
purpose

Challenge of Decision Aggregation



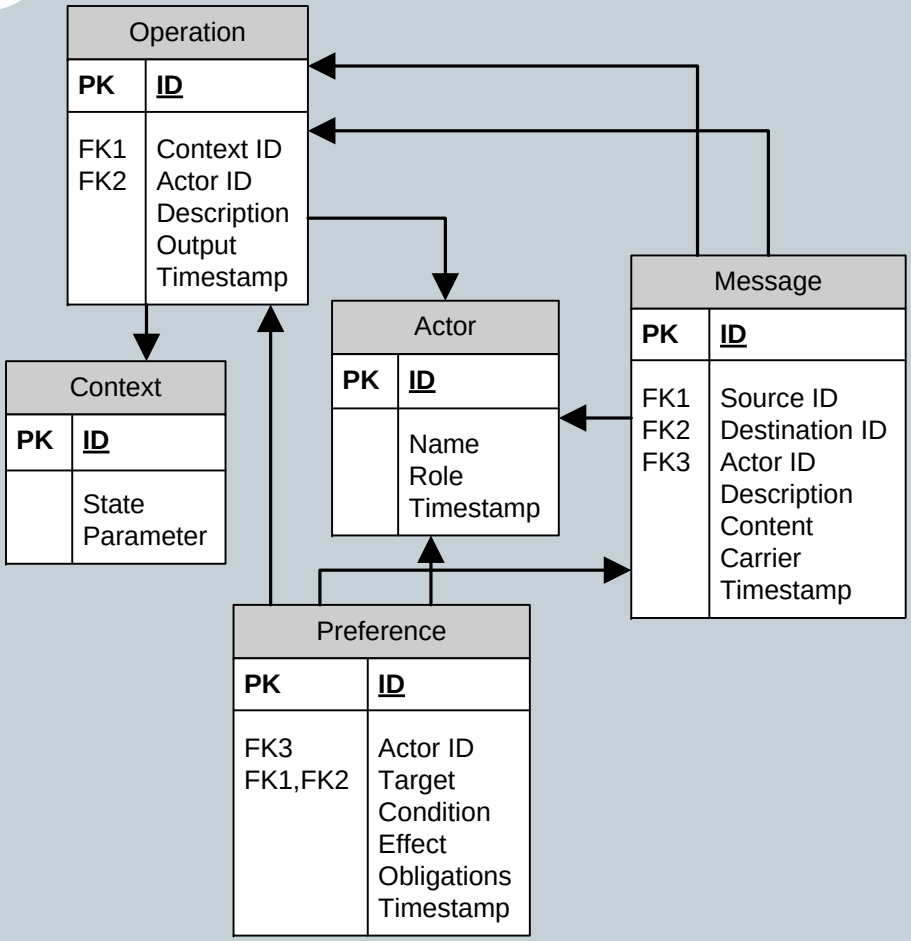
A General Provenance Model

- To understand the requirements of an access control model on provenance, we need understand the data model of provenance first.

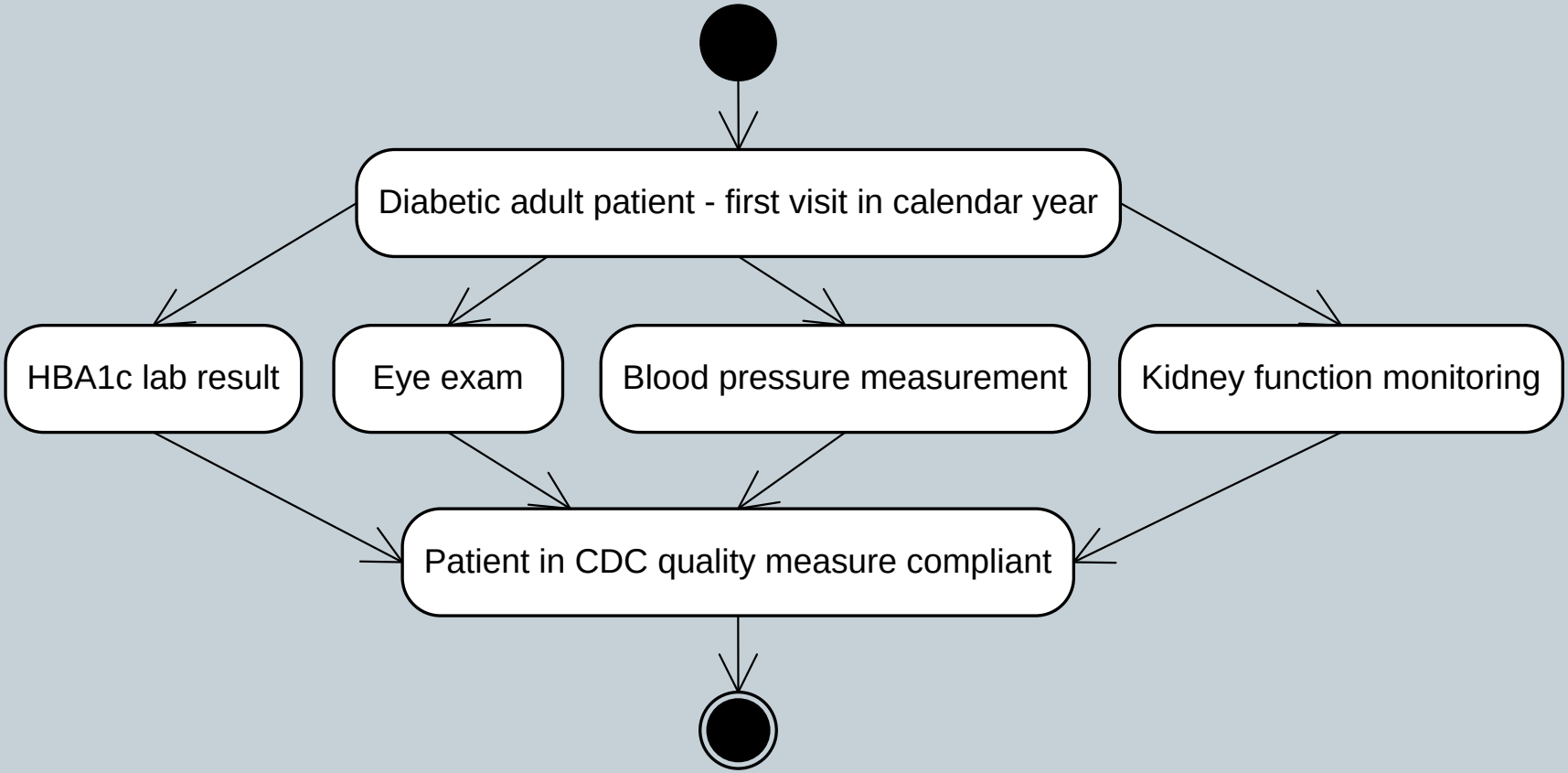


The Schemata of Provence Records

- Provence records
  - Operation records
  - Context records
  - Actor records
  - Message records
  - Preference records



A Healthcare Example



Medical records

Register

ID	Name
1	Alice
2	Bob

Eye_exam

ID	Patient ID	Retinopathy
3	1	Yes
4	2	No

HBA1c

ID	Patient ID	Result
7	1	6.50%
8	2	8.30%

Blood_Pressure

ID	Patient ID	Result
2	1	125-85
3	2	144-95

Kidney_Function

ID	Patient ID	Compliant
5	1	Yes
6	2	No

CDC

ID	Patient ID	Status
8	1	Good
9	2	Bad

Provenance records

Operation

ID	Actor ID	Context ID	Description	Output.record	Output.id	Timestamp
1	1	null	registration	Register	1	1/23/2009 6:00
2	1	null	registration	Register	2	1/24/2009 6:14
3	2	null	eye examination	Eye_exam	3	1/25/2009 6:28
4	2	null	eye examination	Eye_exam	4	1/26/2009 6:43
5	5	null	HBA1c test	HBA1c	7	1/27/2009 6:57
6	5	null	HBA1c test	HBA1c	8	1/28/2009 7:12
7	4	null	Blood pressure	Blood_pressure	2	1/29/2009 7:26
8	4	null	Blood pressure	Blood_pressure	3	1/30/2009 7:40
9	3	null	Kidney function	Kidney_Function	5	1/31/2009 7:55
10	3	null	Kidney function	Kidney_Function	6	2/1/2009 8:09
11	6	null	CDC	CDC	8	2/2/2009 8:24
12	6	null	CDC	CDC	9	2/3/2009 8:38

Actor

ID	Name	Role
1	Jame	Nurse
2	Katty	Practitioner
3	John	Doctor
4	David	Nurse
5	Tom	Practitioner
6	Betty	Doctor

Message

ID	Actor ID	Carrier	Description	Content.record	Content.id	Timestamp	Src ID	Des ID
1	1	paper	Eye exam req	null	null	1/23/2009 8:24	1	3
2	1	paper	Eye exam req	null	null	1/24/2009 8:52	2	4
3	1	paper	HBA1c test req	null	null	1/25/2009 9:21	1	5
4	1	paper	HBA1c test req	null	null	1/26/2009 9:50	2	6
5	1	paper	Blood pressure req	null	null	1/27/2009 10:19	1	7
6	1	paper	Blood pressure req	null	null	1/28/2009 10:48	2	8
7	1	paper	Kidney function req	null	null	1/29/2009 11:16	1	9
8	1	paper	Kidney function req	null	null	1/30/2009 11:45	2	10
9	2	email	Eye exam result	Eye_exam	3	1/31/2009 12:14	3	11
10	5	email	HBA1c test result	HBA1c	7	2/1/2009 12:43	5	11
11	4	email	Blood pressure	Blood_Pressure	2	2/2/2009 13:12	7	11
12	2	email	Eye exam result	Eye_exam	4	2/3/2009 13:40	4	12
13	5	email	HBA1c test result	HBA1c	8	2/4/2009 14:09	6	12
14	4	email	Blood pressure	Blood_Pressure	3	2/5/2009 14:38	8	12
15	3	email	Kidney function	Kidney_Function	6	2/6/2009 15:07	10	12
16	3	email	Kidney function	Kidney_Function	5	2/7/2009 15:36	9	11

Preference

ID	Actor ID	Target. Subject	Target. Record	Target. Restriction	Condition	Timestamp	Effect	Obligs
1	3	actor	operation	actor.role = doctor and operation.id = 10	purpose = research	1/23/2009 6:00	necessary permit	null
2	5	actor	operation.body	operation.id = 5 and actor.name = David	null	1/27/2009 6:57	deny	null
3	3	actor	message.body	message.id = 16	purpose= marketing	2/7/2009 15:36	deny	null

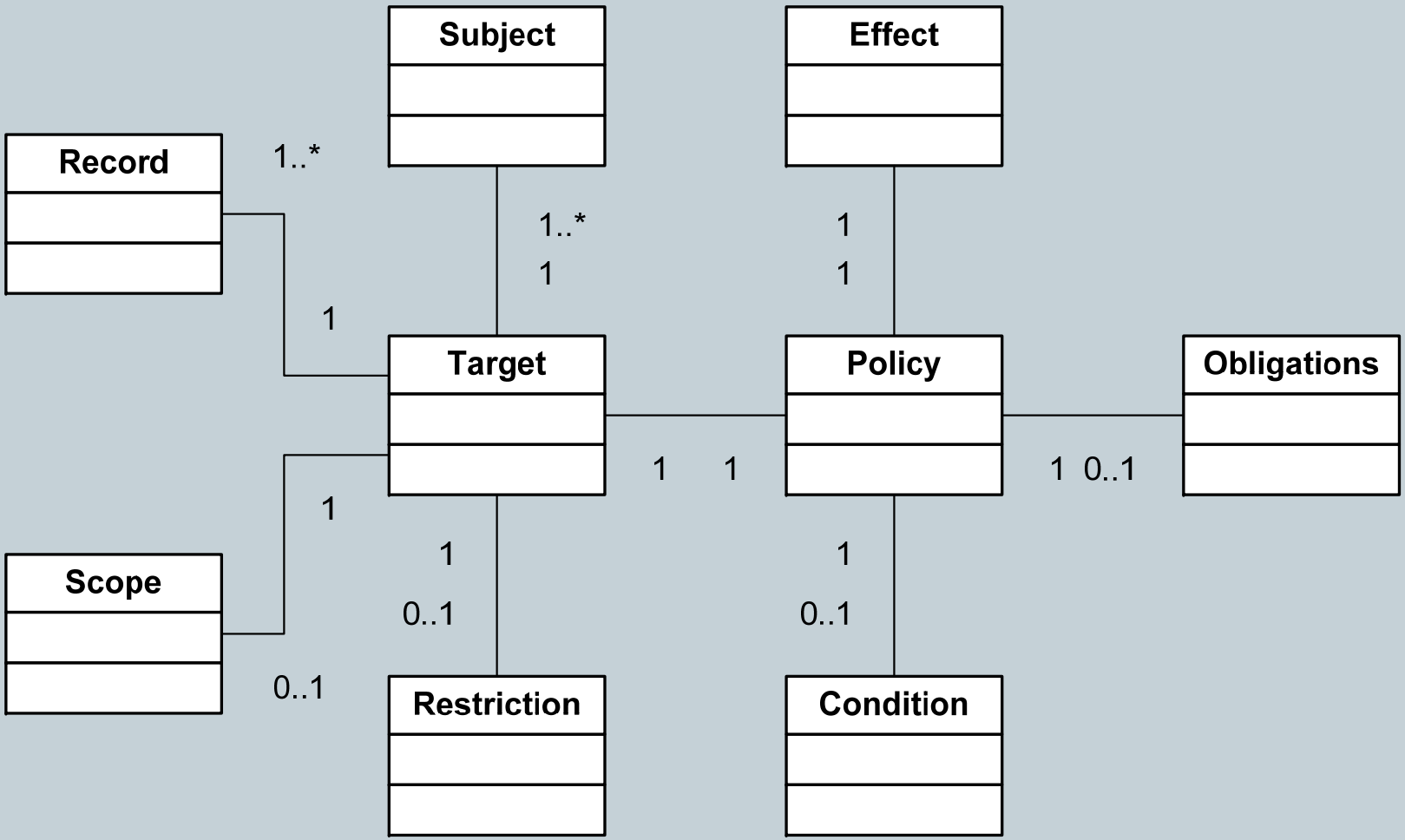
Observations

- Each medical record is generated by one operation at a specific time, and can be uniquely identified by the output attribute (with two fields) in the operation's record.
- Some message records have values in their content attributes that reference medical records, and others do not.
- Message records and operation records connected by these message records form two independent DAGs whose structure is exactly the same as that of the workflow of interest.
- Actor records are referenced from operation, message, and preference records.
- Each preference record references exact one message record or operation record.

Desiderata for an Access Control Model

- First, provenance access control must be fine-grained.
- Second, provenance access control may have to constrain data accesses in order to address both security and privacy.
- Third, provenance access control may need both originator control (ORGCON) and usage control (UCON).

The Language Model



Target

- The target specifies the set of subjects and records, to which the policy is intended to apply.

```
<target>
  <subject>anyuser</subject>
  <record>operation.description</record>
  <restriction>anyuser.role == doctor AND
  operation.timestamp <=1.1.2009</restriction>
</target>
```

Condition

- A condition represents a boolean expression that describes the optional context requirements that confine the applicable access requests, e.g. access purpose, limitation on access time and location, and verification of the record originator's license.

<condition>system.machineid == obelix AND purpose == research</condition>

Obligation

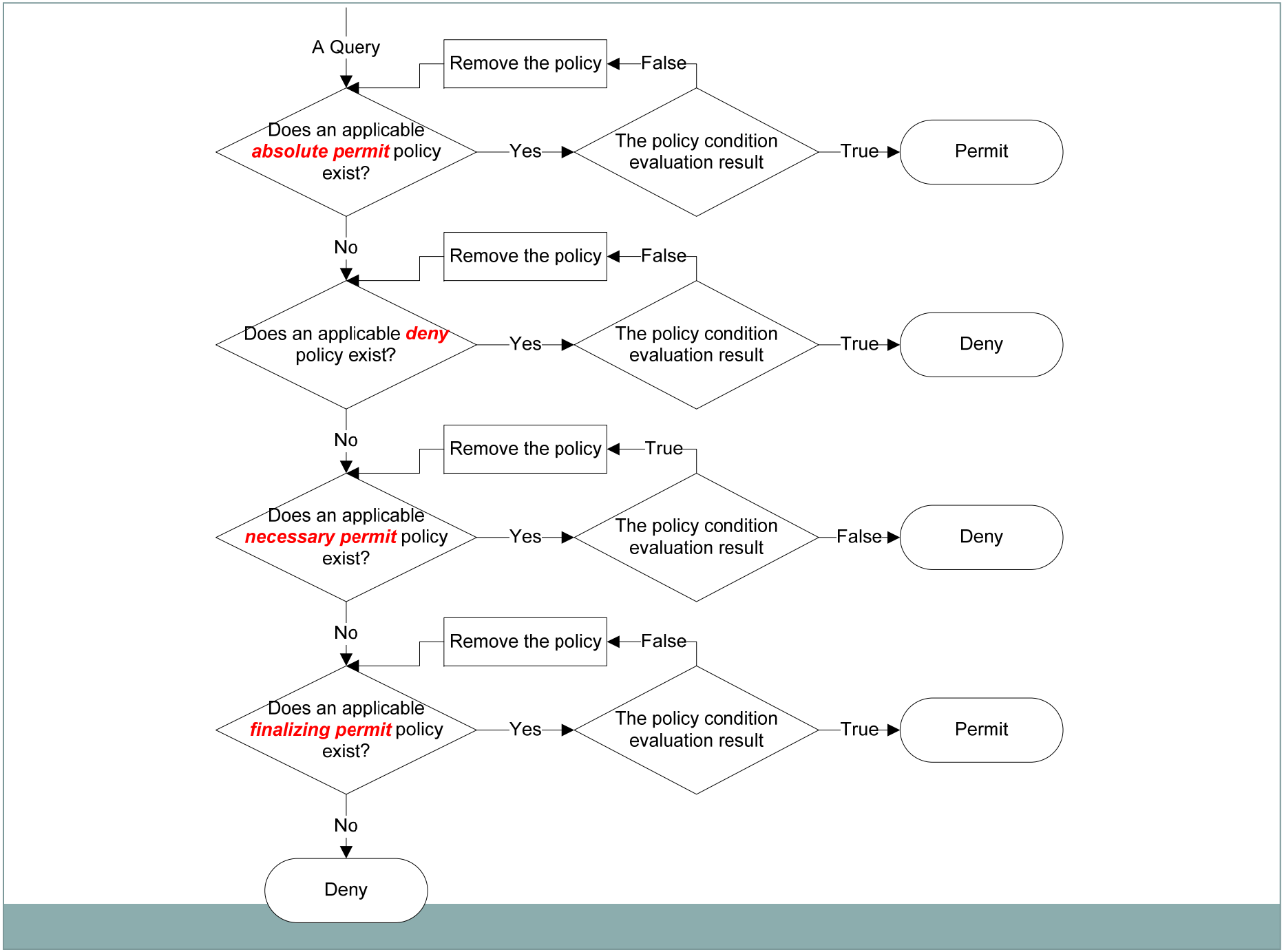
- An obligation is an operation, specified in a policy, that should be executed before the condition in the policy is evaluated, in conjunction with the enforcement of an authorization decision, or after the execution of the access.

```
<obligations>
   <obligation>
         <operation>inform the actor of the record</operation>
         <temporal constraint>10 days</temporal constraint>
         <fulfill on>access</fulfill on>
   </obligation>
</obligations>
```

Effect

- The effect of a policy indicates the policy author's intended consequence of a "true" evaluation for policy: *Absolute Permit*, *Deny*, *Necessary Permit*, and *Finalizing Permit*.

```
<policy ID=1>
  <target>
    <subject>anyuser</subject>
    <record>operation.description</record>
    <restriction>anyuser.role == doctor AND operation.timestamp < 1.1.2009</restriction>
  </target>
  <condition>system.machineid == obelix AND purpose == research</condition>
  <effect>necessary permit</effect>
</policy>
```


A Query
Remove the policy
False
Does an applicable absolute permit policy exist?
Yes
The policy condition evaluation result
True
Permit
No
Remove the policy
False
Does an applicable deny policy exist?
Yes
The policy condition evaluation result
True
Deny
No
Remove the policy
True
Does an applicable necessary permit policy exist?
Yes
The policy condition evaluation result
False
Deny
No
Remove the policy
False
Does an applicable finalizing permit policy exist?
Yes
The policy condition evaluation result
True
Permit
No
Deny

Originator Preference

- The access control language can be applied to specify originator preferences, that is, to support originator control.

```
<preference ID=1>
   <target>
         <subject>anyuser</subject>
         <record>operation.description</record>
         <restriction>operation.ID == 12345678</restriction>
   </target>
   <condition> purpose == reverse engineering OR purpose == reselling</condition>
   <effect>deny</effect>
   <timestamp>1.29.2009</timestamp>
</preference>
```

Purpose Binding

- In conjunction with effects, purpose predicates can directly model the following common cases of purpose requirements in privacy regulations.
  - some records can only be used for some specific purposes;
    - <condition>purpose == research OR purpose == development</condition>
    - <effect>necessary permit</effect>
  - some records can be used for some specific purposes;
    - <condition>purpose == research OR purpose == development </condition>
    - <effect>finalizing permit</effect>
  - some records should not be used for some purposes.
    - <condition>purpose == marketing</condition>
    - <effect>deny</effect>

Additional Examples

- The language can be applied to examples proposed by other approaches, e.g. Braun et al. and Hasan.
  - Employee Performance Review
    - <policy ID=1>
      - <target>
      - <subject>anyuser</subject>
      - <record>operation</record>
      - <restriction>operation.output.record == review AND anyuser.name == review.objectname</restriction>
      - </target>
      - <effect>deny</effect>
    - </policy>

Conclusion and Future Work

- In the evaluation of provenance access control policies, decisions with uncertainties about the result of target evaluation or condition evaluation may arise.
- Delegation of access control rights, which is one important requirement for provenance access control has not been addressed in this paper.
- Because of the semantics of different effects and predicates used in conditions and restrictions, inappropriate policy specifications may generate conflicting policies or redundant policies.

Questions