Purpose Management and Enforcement for Sensitive Private Data in Open Environments

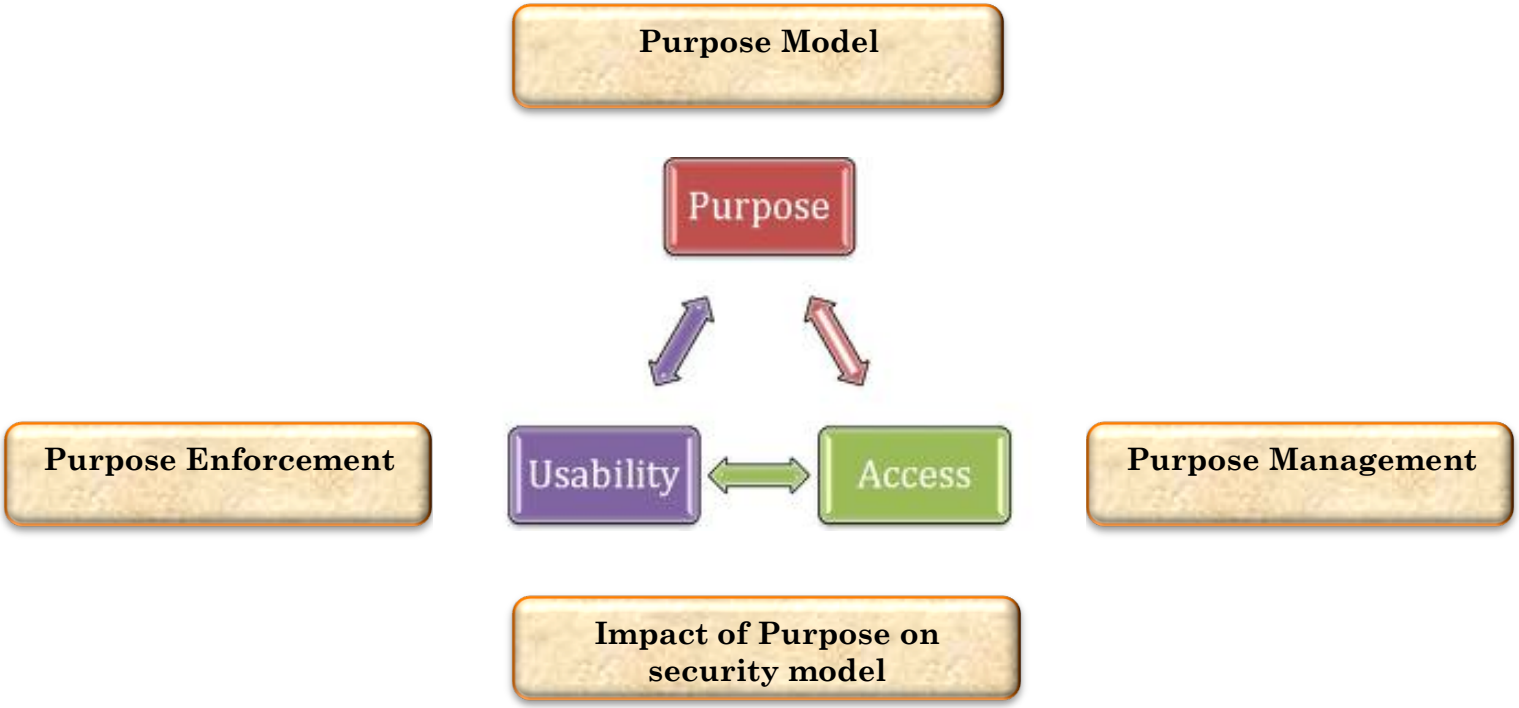
Presented by: Mr. Annanda Th. RATH
Faculty of Computer Science, University of Namur, Belgium.

Presentation Plan

- Research objectives
- Methodological consideration
- Application domains
- Purpose modeling
  - Definition and scope
  - Purpose under the context of privacy policy
- Purpose management and enforcement
  - Purpose enforcement structure
- Work done so far
- Ongoing-work
- Future work
  - Purpose in the context of relationship-based access control model
- Conclusion

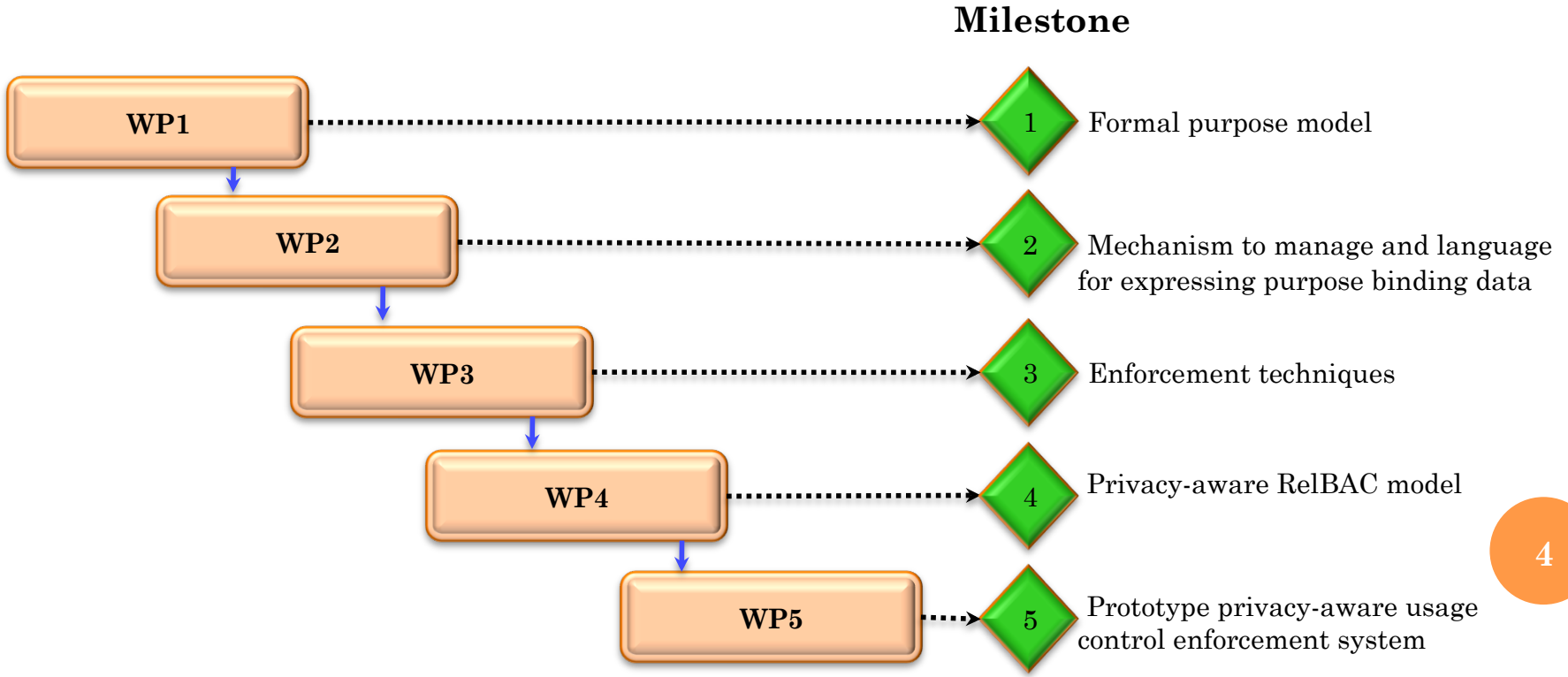
Research Objectives

- The goal of the research is to investigate the role and impact of ”purpose” in authorization process (access as well as usage control) and define a mechanism to manage and enforce them.
- The research includes:
  - (1) study, analyze, and clear the meaning of purpose.
  - (2) management of purpose binding of data.
  - (3) study the possibilities to recognize purpose binding and enforcement.
  - (4) clear the meaning and impact of personal relationship, context on purpose in authorization process.



METHODOLOGICAL CONSIDERATIONS

- WP1: define the definition and scope of purpose
- WP2: define a mechanism to manage purpose in open environment
- WP3: work on purpose enforcement structure
- WP4: impact of purpose on access control to private data
- WP5: prototype: tools



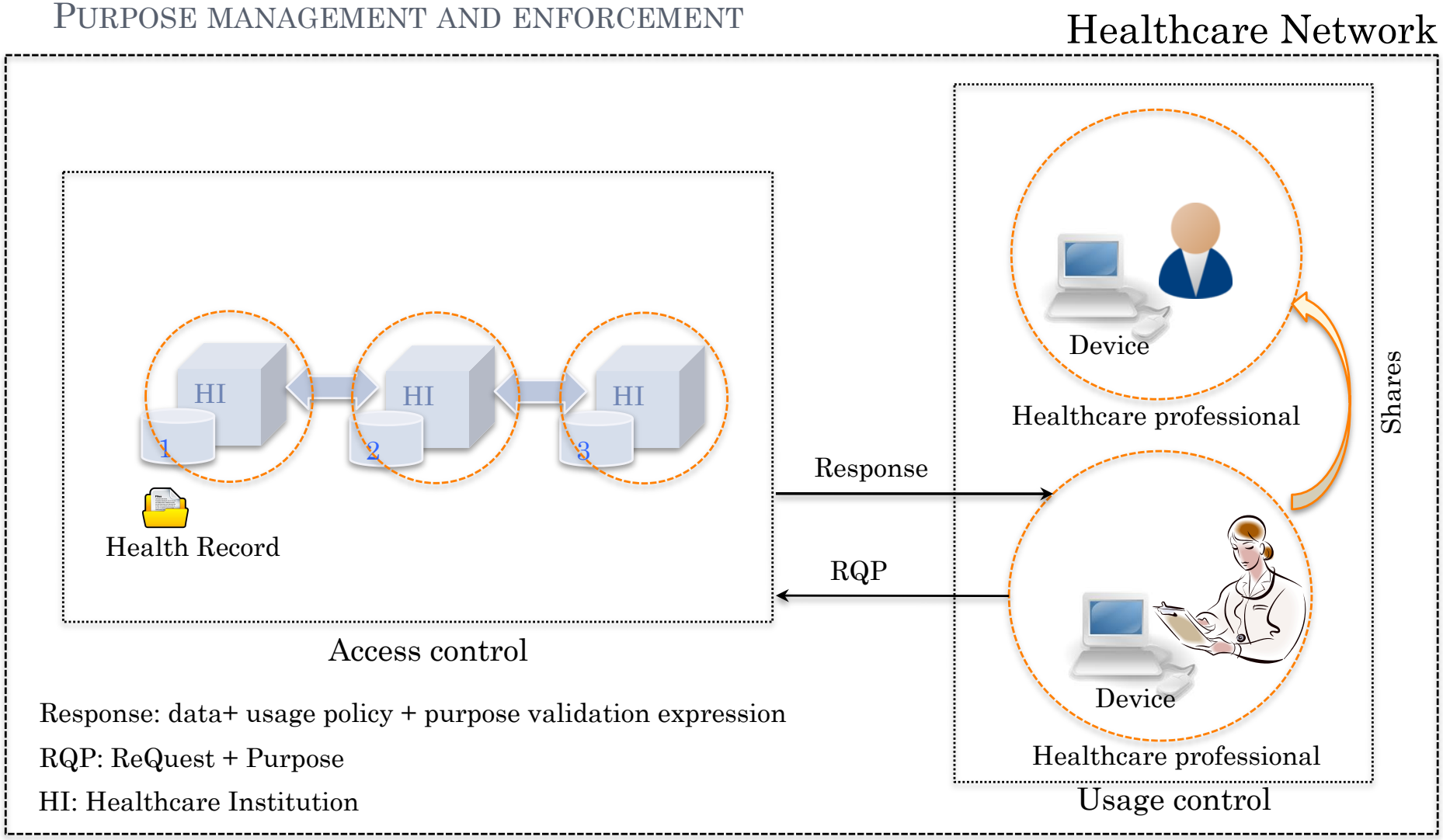
WP: Work Package, RelBAC: Relationship-Based Access Control

Focus domains

- Application domains
  - Distributed healthcare
  - Facebook-like social network
- Our focus at this stage
  - Distributed healthcare
    - Modeling the purpose, its management and enforcement.
  - For Facebook-like social network
    - Study the impact of purpose on the access control based on relationship between data owner and requester.
    - Define a model based on the relationship in the context of sensitive private date.

Motivating example

Purpose management and enforcement



Requirements:

1. Health record can reside on user's device for limited period of time.
2. It can be shared among healthcare professionals
3. The permission allowed to reuse the record depending on the current state of purpose validation, not the validity of the purpose at the time of first access/request.

Purpose

Definition and scope

What

is purpose

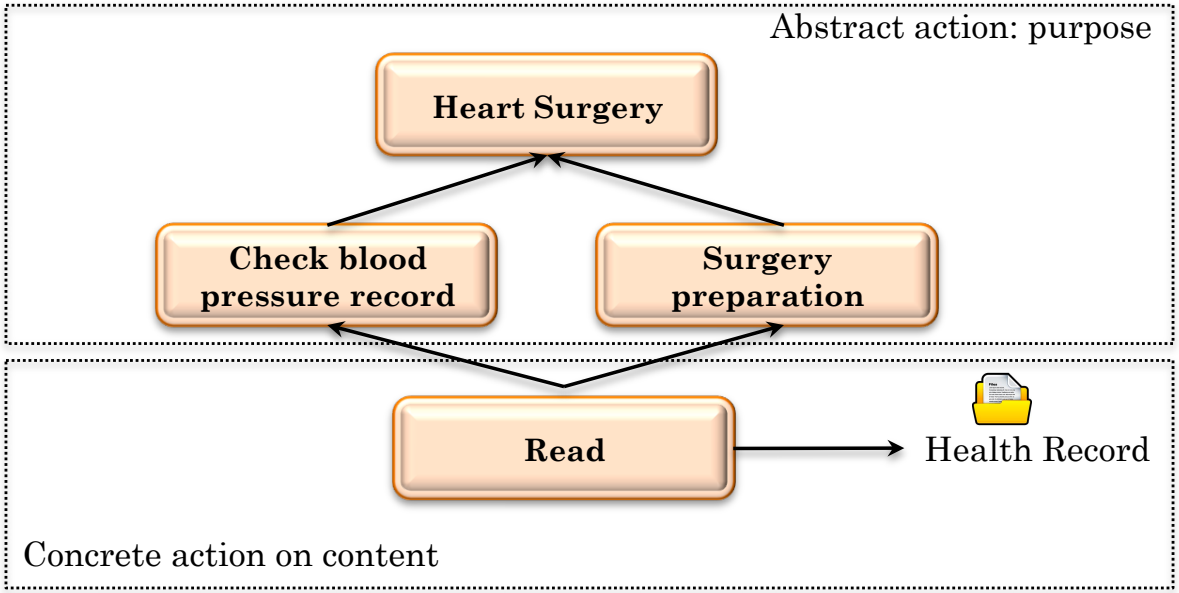
?

Purpose

- Definition: in dictionary, "purpose" is defined as "the object toward which one strives or for which something exists; an aim or a goal".
  - But by observing how purpose is used in the natural language reveals that purposes often refer to an or a set of abstract actions.
  - Example: accessing patient's health record for the purpose of treatment, research, insurance, etc.
  - Purpose can be classified in two types:
    - Purpose as high-level action
    - Purpose as future action

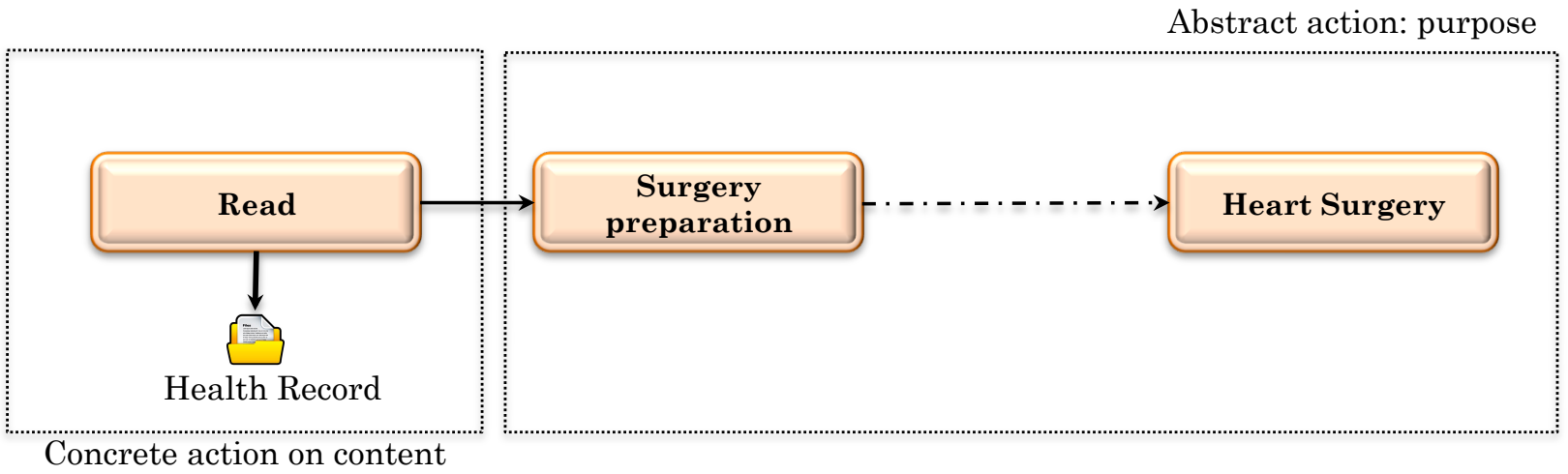
Purpose as high level action

- Definition: in some contexts, purpose refers to a more abstract, or semantically higher-level action in a plan. Thus, doing something for some purpose, actually means doing it as a part, or a sub-action, for that higher-level action.
  - Example, when Bob checks some patient's blood pressure record for the purpose of heart surgery.



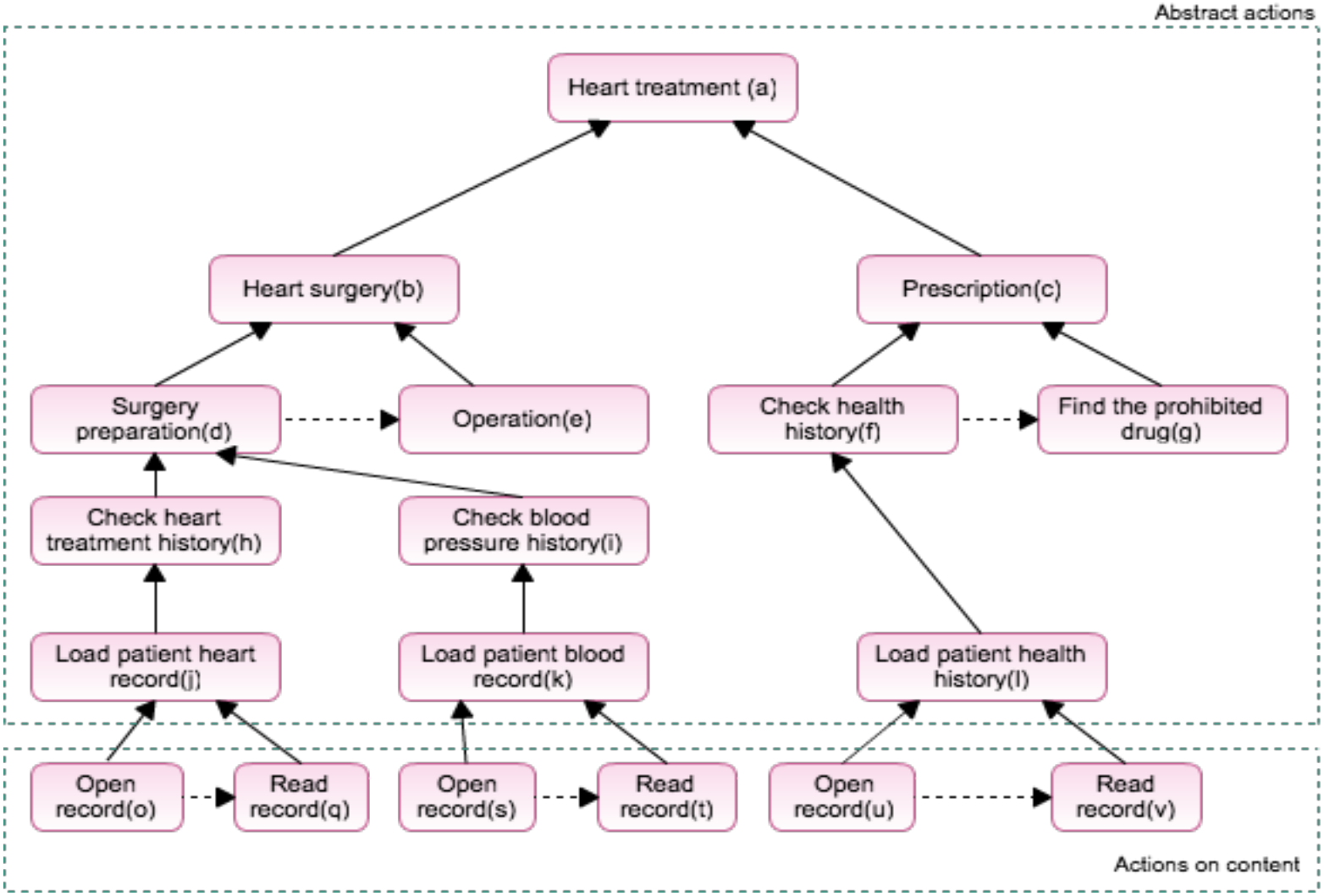
Purpose as future action

- Definition: in some contexts, purpose is used to indicate that an action is performed as a prerequisite of another action in future.
  - Example, when Bob withdraws money from a bank account for the purpose of paying the bills, it means the former action is done as a prerequisite to performing the latter.



Motivating example

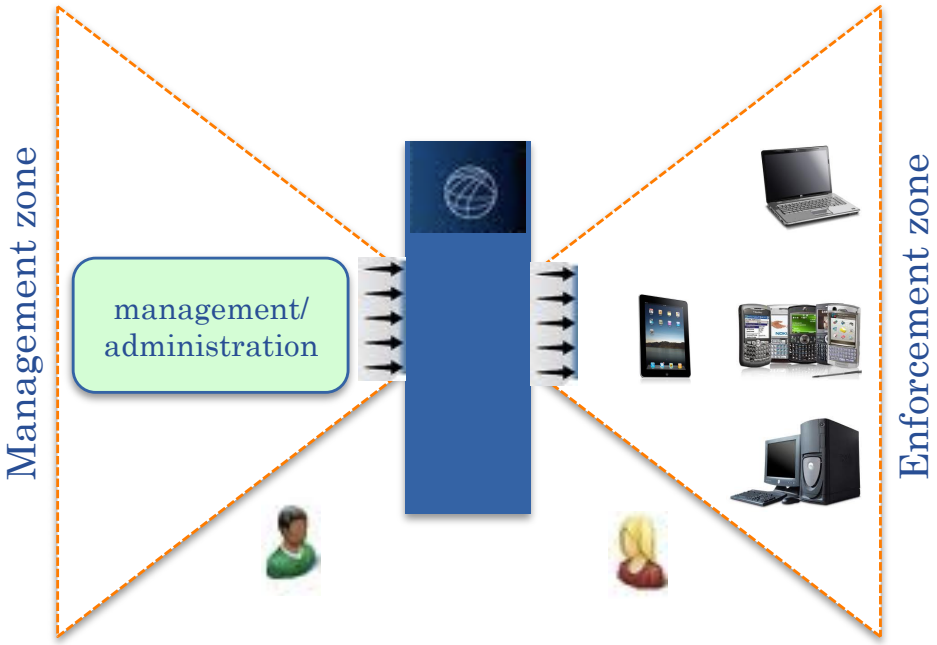
- Purpose model for healthcare information system.



Purpose tree

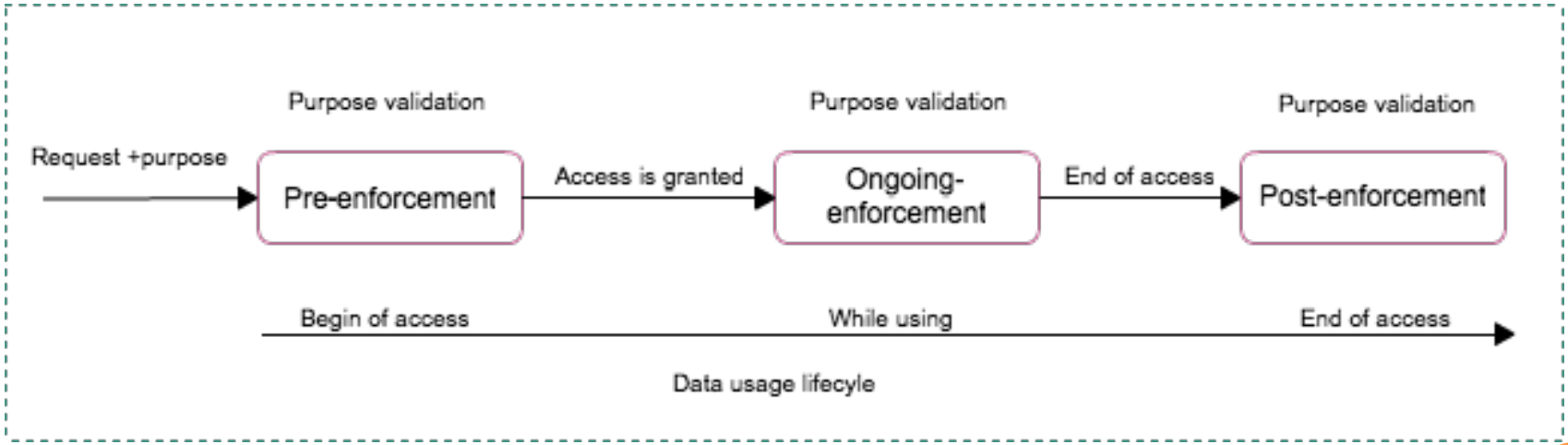
PURPOSE ENFORCEMENT

UNDER THE CONTEXT OF USAGE CONTROL



Purpose enforcement structure

- Enforcing "purpose" means to verify that those abstract actions exist and they are valid before data is released to requester and in some contexts, they need also to be valid during the usage of data.
- Purpose enforcement structure
  - Pre-enforcement
  - Ongoing-enforcement
  - Post-enforcement



PRE-ENFORCEMENT OF PURPOSE

- Requirements
  - System needs to validate if the purpose claimed by requester is existed and valid.
- Existing enforcement mechanisms
  - Allow agent to explicitly announce the purpose of data access
  - Use role-based enforcement, where purpose is aligned to role of user.
- Limitation
  - Anyone can claim any purpose of access, without the proper system to validate claimed purpose, this method can not be used in data processing environment like distributed healthcare.
  - Roles and purposes are not always aligned and members of the same organizational role may practice different purposes in their actions.
- Conclusion
  - Identifying the purpose of action or verifying the claimed purpose remains an open question.

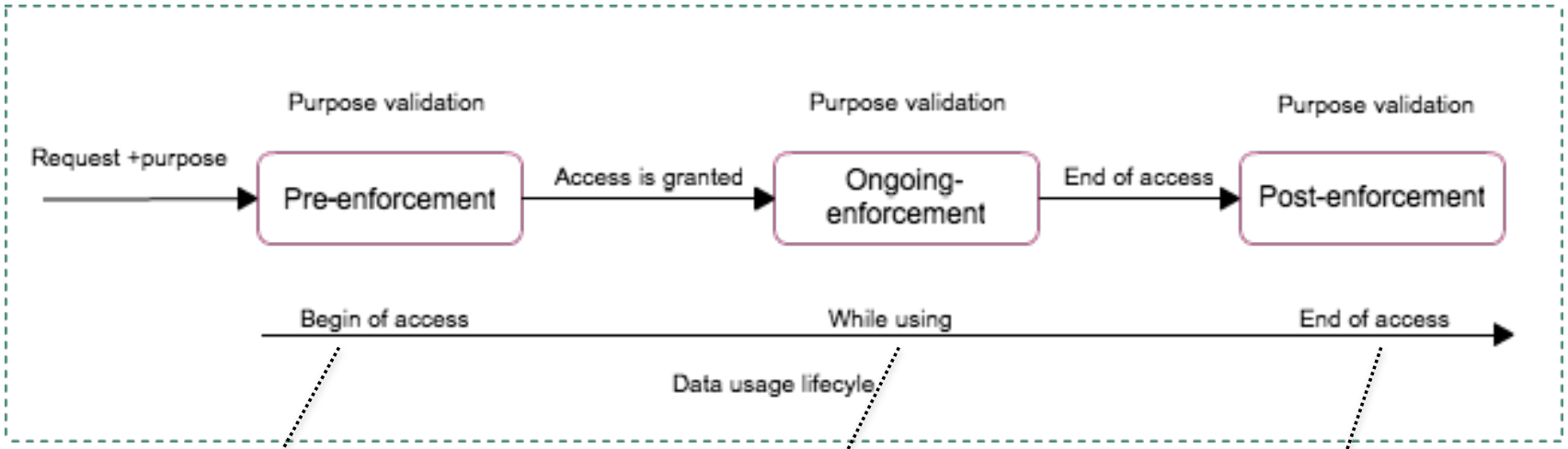
ONGOING-ENFORCEMENT OF PURPOSE

- Requirements
  - System needs to validate if the purpose claimed by requester is existed and valid and continues to be valid during the usage session.
  - All the actions performed, being performed, and performing on data during usage session must be conformed with the claimed purpose.
  - System needs to trigger the purpose re-evaluation periodically during usage session.
- Existing enforcement mechanisms
  - Rule-based or workflow, where purpose is attached with rule or a workflow, which defines a sequence of allowed actions during usage of data.
- Limitation
  - The workflow-based enforcement does not work with the purpose that does not have the natural interpretation of workflow. Example, "research purpose or statistic" in the context of healthcare system.
- Conclusion
  - It remains an interesting work to find an effective enforcement mechanism to fill the missing gape. That refers to "purposes" that do not have the natural interpretation of workflow.

POST-ENFORCEMENT OF PURPOSE

- Requirements
  - All the performed actions on content need to be complied with claimed purpose.
- Existing enforcement mechanisms
  - Rule-based, workflow-based, and logging. The idea is to analyze the usage-log based on the defined rule. The logical reconstruction of execution process can be used to compare with the data access rule and the defined flow of actions and find out if user violated the claimed purpose or not.
- Limitation
  - The workflow-based enforcement does not work with the purpose that does not have the natural interpretation of workflow.
  - It is the pro-active method.
- Conclusion
  - It is still interesting to find other enforcement mechanism that can be used for all types of purpose.

PURPOSE ENFORCEMENT



Agent explicitly announce purpose of usage	**Rule-based enforcement**	**Workflow + usage-log**
Role-based enforcement	**Workflow-based enforcement**	**Rule + usage-log**
New mechanism ????	**New mechanism ????**	**New mechanism ????**

Research on purpose enforcement

- What are important things that need to be done:
  - Purpose management
    - Study existing management models applied in private data processing environment.
    - Study the existing right/policy expression language to find out whether those languages support the purpose expression or not. This is in the context of usage control.
    - Study the existing system infrastructure, if they are sufficient to handle the management of purpose in a complex and high security demand data processing environment like distributed healthcare.
  - Purpose enforcement
    - Study the existing purpose enforcement model and categorizing them according to our proposed enforcement structure.
    - Find out what are the weakness and strengths of those models.
  - Define an expression mechanism for purpose validation
    - The idea is to formalize the expression language for expressing how purpose should be validated in an open environment. Do not confuse with usage policy expression (UPE). UPE expresses how data should be processed while purpose validation, it expresses how purpose should be validated.

WORK DONE SO FAR

Work: Chronological order

- Case study on Walloon Healthcare Network (WHN)
- Survey on DRMs system and technologies
- Study different right/policy expression languages
- Study of “purpose”, this includes the semantic foundation of purpose for privacy policies to access control model based on purpose and its expression language.
- Survey on purpose enforcement techniques
- Define a purpose enforcement model for usage control applied in distributed healthcare.

Survey on existing technologies

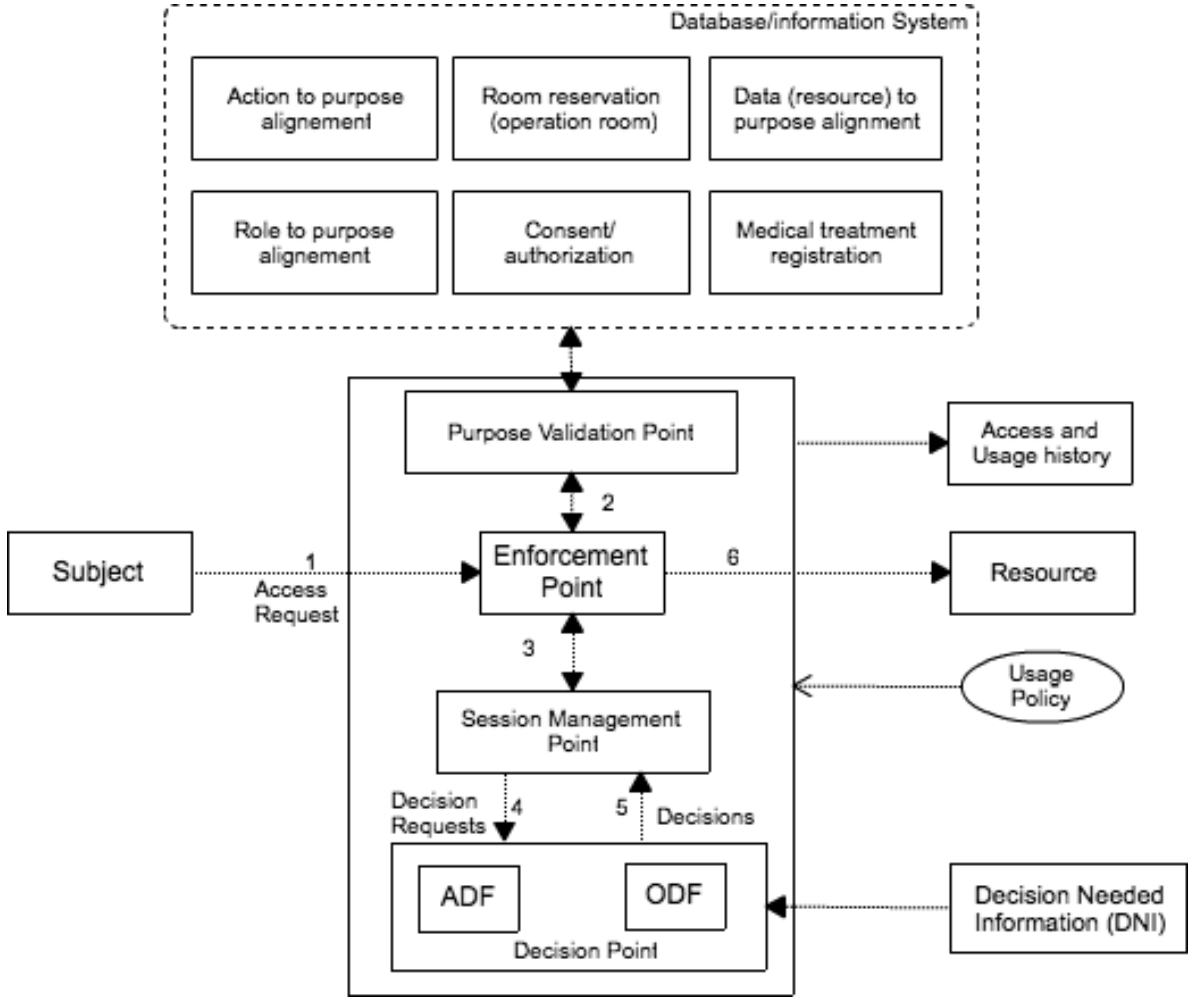
- Right expression language
  - XACML
  - EPAL
  - ODRL
  - etc ..
- Purpose enforcement techniques
  - Rule-based enforcement
  - Role-based enforcement
  - Workflow-based enforcement
- Access and usage control model
  - MAC, DAC, RBAC, P-RBAC, purpose-based access control, etc
  - UCON (Usage CONtrol)

PURPOSE MODEL

- Defined scope and definition of purpose.
- Study the impact of “Purpose” on security for private data.
- Study the role of “Purpose” in legislation concerning the processing of private data.
- Model the purpose for distributed healthcare.
- Proposed a purpose-based usage control enforcement model for distributed healthcare.

Purpose enforcement model

- Toward enforcement of purpose for privacy policy in distributed healthcare



Purpose-based usage control enforcement model

ONGOING-WORK

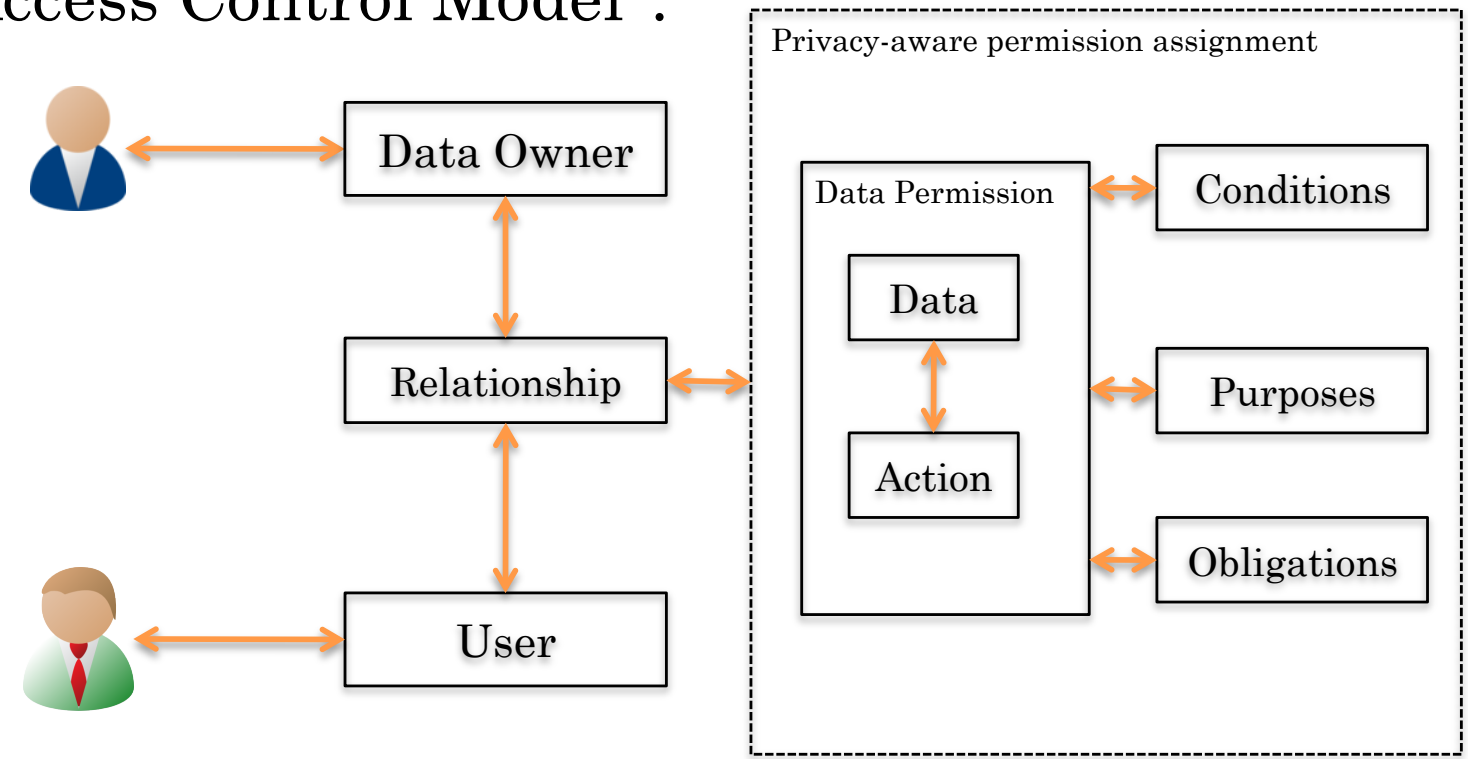
Purpose enforcement

- Expressing purpose/hierarchical purpose in right/ policy expression language.
- Purpose validation expression
  - Define a formal language for expressing how purpose should be validated in open environment.
  - Extending the work to hierarchical purpose.
- Purpose enforcement
  - Define an enforcement technique for ongoing-enforcement and post-enforcement of purpose.

FUTURE WORK

THE IMPACT OF PURPOSE

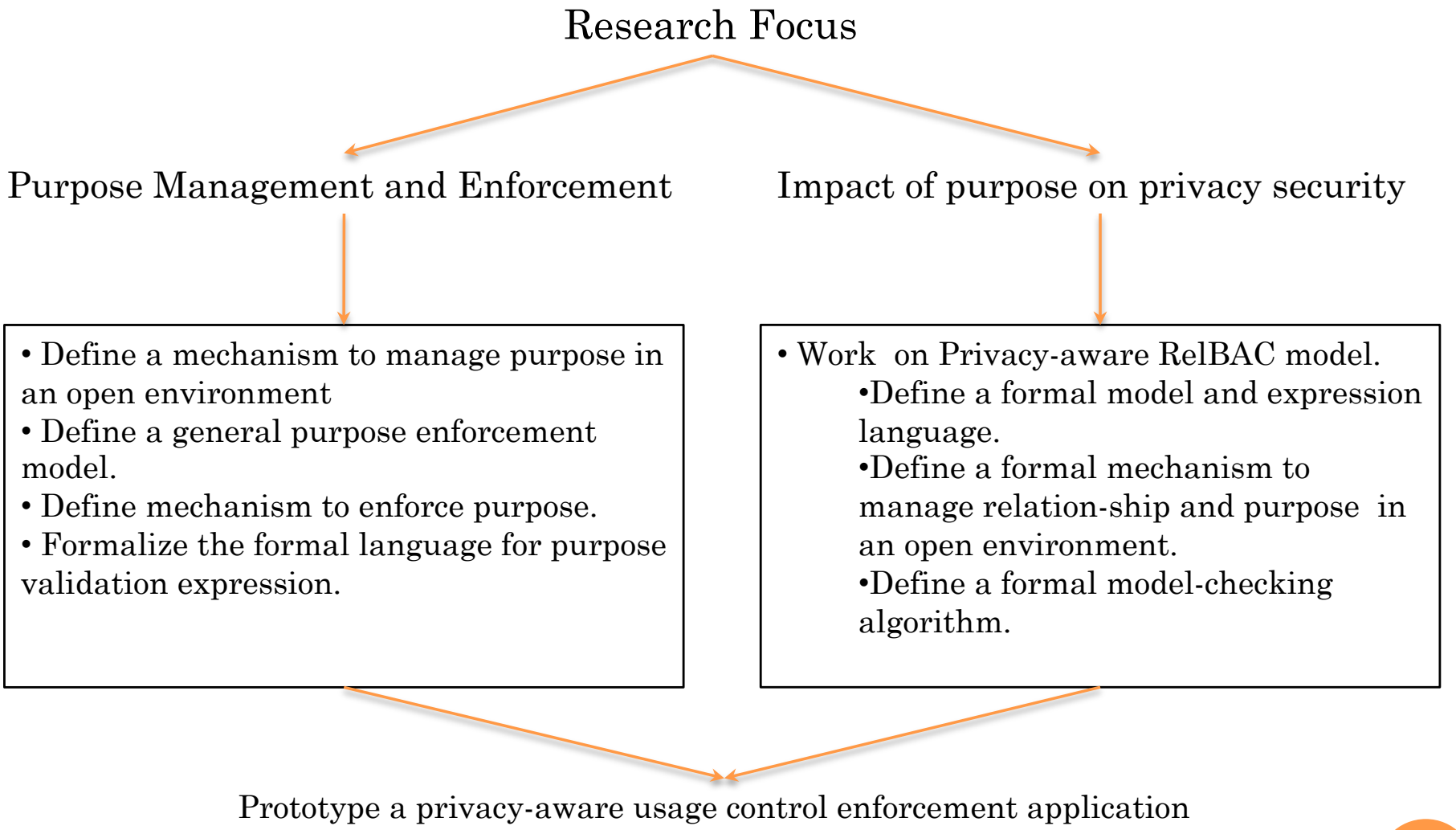
- The aim is to study the impact of purpose on the security model dealing with private data.
- We investigate a model that bases on the relationship between data owner and requester, we term "Privacy-aware Relationship-based Access Control Model".



Research on P-RelBAC

- Define a proper model and expression language.
- Introduce the concept of purpose we identified so far and most importantly the hierarchical purpose.
- Extend this model to be used in distributed environment.
  - How to manage the relation of user and purpose of access in open environment.
  - Investigate the enforcement techniques for this proposed model when deploying it in an open environment.

SUMMARY: RESEARCH FOCUS



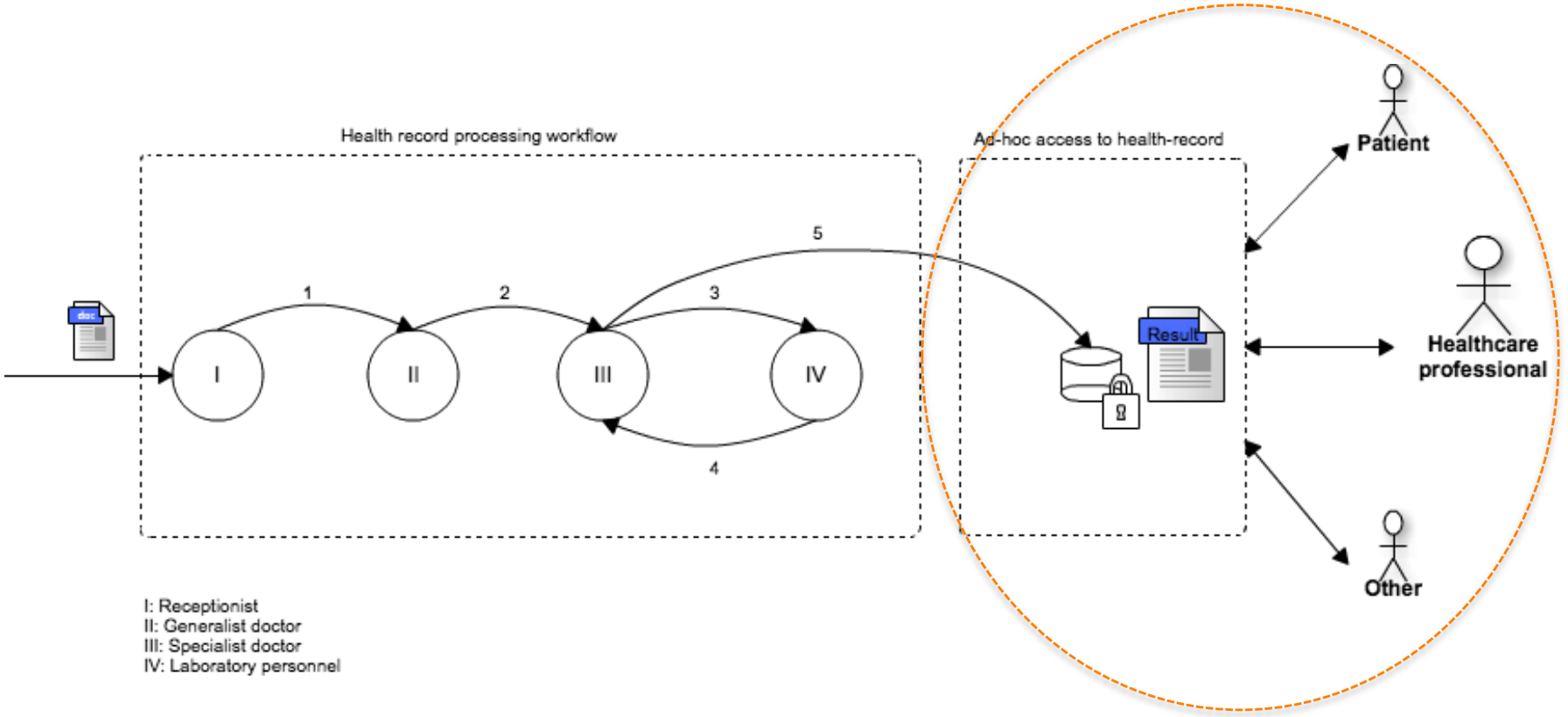
Conclusion

- Focus on purpose management and enforcement in open environment.
- First phase of our research focused on defining the scope and meaning of purpose as well as its model.
- We proposed the purpose enforcement structure and our preliminary conclusion is that with the proposed-structure, we would have a promising result for "purpose" enforcement in usage control context.
- We designed the usage enforcement model that encompasses "purpose" for distributed healthcare.
- Up to this state we studied and defined the system model and requirements, surveyed on existing technologies, and model the first purpose-based usage control system designed for distributed healthcare.
- Although, many works have been done, a lot more are awaiting to be done in order to reach our defined research goal.

Thanks

Questions ?

General workflow for e-health



Scenario: Health check concerning blood sample

Patient visits receptionist/assistant with his dossier

1: Dossier is forwarded to generalist doctor.

3: Generalist doctor identified the illness and forwards the dossier to specialist doctor

3: Specialist doctor forwards the documents and blood sample to laboratory personal for the test

4: After the test the result is sent to specialist doctor for the approval

5: The result is recorded and stored in data for future use.

EXAMPLE: PURPOSE VALIDATION EXPRESSION

PU = (P, WHEN, DURATION, VALIDATION)

- "P" is a purpose of data usage claimed by subject.
- " WHEN" tells when the purpose should be check, it can be "pre, ongoing, or post".
- "DURATION" is the time period to check the validation of purpose (e.g., during the emergency treatment session).
- "VALIDATION" expresses the mechanism used to check the validity of the purpose claimed by subject.

```
<purpose-validation function= "any-of">
      <purpose type="hierachicalType"  purpose-name="heart-surgery">
            <purpose-when datatype="String">pre-enforcement </purpose-when>
            <purpose-duration datatype="TimeInterval"> time-period</purpose-duration>
            <purpose-mechanism MatchId="role-to-purpose alignment"> validation-mechanism
            </purpose-mechanism>
      </purpose>
      <purpose type="hierachicalType"  purpose-name="heart-surgery">
            <purpose-when datatype="String">pre-enforcement </purpose-when>
            <purpose-duration datatype="TimeInterval"> time-period</purpose-duration>
            <purpose-mechanism MatchId="action-to-purpose alignment"> validation-mechanism
            </purpose-mechanism>
      </purpose>
      ----------
</purpose-validation>
```