RQ5: Automating regulatory constraints and data governance in healthcare

EPI Quarterly Meeting

Milen G. Kebede . 07.04.2022
Supervisors: Prof. Tom van Engers, Dr. Thomas Binsbergen, Dr. Dannis van Vuurden

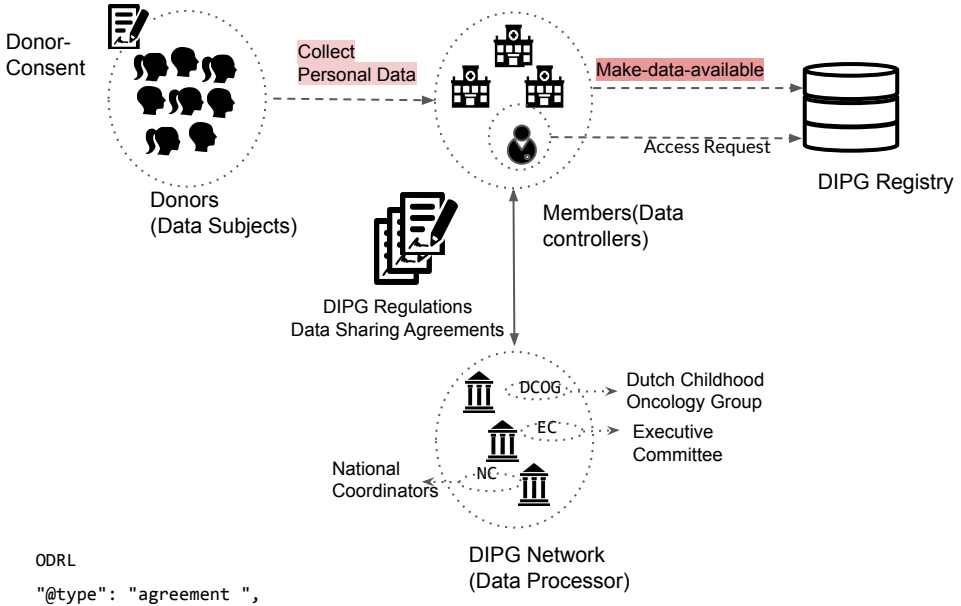
Overview

Research Objective: formalising wide variety of normative sources such as regulations and contract to automate the required monitoring , control and enforcement of such norms.

Diffuse Intrinsic Pontine Gliomas(DIPG) registry: rare disease repository that allows researchers to access patient data that can lead to discovering new treatment and prognosis factors.

Our work so far: Identifying requirements from **legal norms**, use-case and **access control mechanisms**

- Policy specification languages
  - Open Digital Rights Language(ODRL)
    - Lack of monotonicity in representing delegation, semantic ambiguity in the usage of ‘Duty’, granularity in identifying parties
  - eFLINT
    - Modular specification & linking social policies with system level policies



ODRL

```
"@type": "agreement ",
 "uid": "ex:policy:00",
 "profile": "ex:odrl:profile:00",
 "permission": [{
   "assigner": "EC",
   "assignee": "member",
   "action": "transfer",
   "target": "datasetA",
```

eFLINT

```
Extend Act make-data-available Syncs with (Foreach donor:
  collect-personal-data(controller = institution
                        ,subject    = donor
                        ,data       = dataset
                        ,processor  = "DCOG"
                        ,purpose    = "DIPG Research")
    When subject-of(donor, dataset))
```

Data Sharing Agreement ontology

To answer questions such as :

- Expressing privacy policies as RDF triples
- Access control policy concepts with the domain concepts

Query the ontology (Compliance questions)

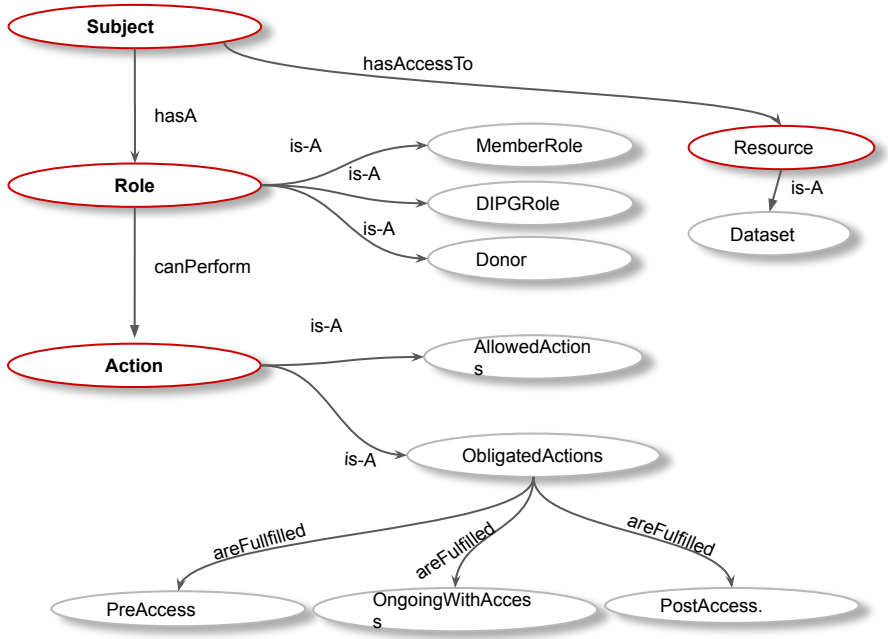
- What obligations does a member need to meet before making data available?
- What Obligations need to be fulfilled before a member accesses the Registry?

End Goal:

- To continue to extend the ontology to identity core concept of DSA for a more generic DSA ontology
- To possibly use the ontology to support policy administration points

Subject predicate Object

The researcher shall use data for approved project only.



eXtensible Access Control Markup Language(XACML)

XACML: a recognized standard for the specification of access control policies

Obligation: An operation specified in a rule, policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision.

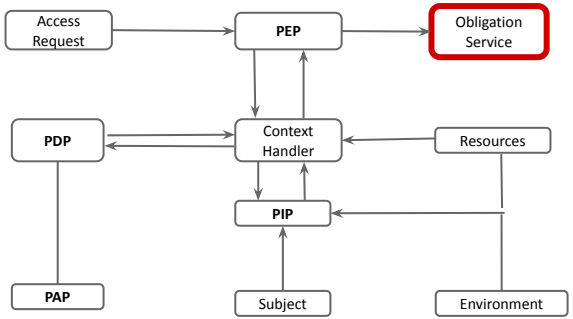
Limitations - Temporal positioning of the obligation with respect to users action, the party that is expected to fulfill the obligation can be different from the subject, PEP is expected to understand what the obligation mean.

Do action *when* {trigger$_1$ V trigger$_2$ V trigger$_n$}

E.g **Do** DeleteDataset () **when** {ProjectExpires(p,t)}

- **Define events that trigger obligations(sharing data to third party(jurisdiction), project start & end..)**

Pre-access : fulfilled before access
Ongoing : need to be fulfilled during usage of resource
Post-access : After access period has passed



XACML architecture components

"Delete data once your project duration expires.

```
<ObligationExpressions>
<ObligationExpression ObligationId="obligation:email" FulfillOn="Deny">
<AttributeAssignmentExpression
AttributeId="attribute:mailto"> <AttributeSelector
MustBePresent="true"
Category="resource" Path="record/researcher/Contact/email"
DataType="XMLSchema#string"/>
</AttributeAssignmentExpression>
<AttributeAssignmentExpression AttributeId="Delete data">
<AttributeValue DataType="XMLSchema#string">Your contract has expired,
therefore, according to the DSA, delete data within three months</
AttributeValue> </AttributeAssignmentExpression>
</ObligationExpressions>
```

Conclusion

Future work: Conflict resolution, Violation Detection, Remediation

- Implementing the policy management system in BRANE

Publications

Kebede, Milen G. "Automating Normative Control for Healthcare Research." *AI Approaches to the Complexity of Legal Systems XI-XII*. Springer, Cham, 2020. 62-72

Kebede, Milen G., Giovanni Sileno, and Tom Van Engers. "*A critical reflection on ODRL*." *AI Approaches to the Complexity of Legal Systems XI-XII*. Springer, Cham, 2020. 48-61

van Binsbergen, L. T., Kebede, M. G., Baugh, J., van Engers, T., & van Vuurden, D. G. (2022). *Dynamic generation of access control policies from social policies. Procedia Computer Science*, *198*, 140-147