RQ5: Automating normative control for Healthcare research

Milen G. Kebede

Informatics Institute, University of Amsterdam
m.g.kebede@uva.nl

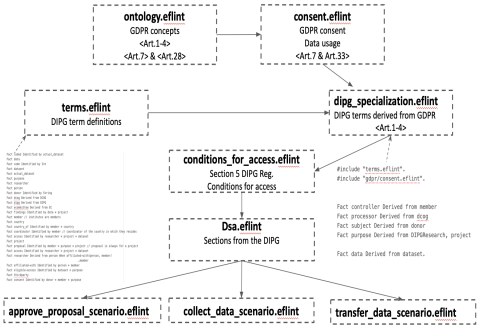
July 1, 2021

Supervisors : Prof. Tom van Engers, Dr. Thomas van Binsbergen, Dr. Dannis van Vuurden

Use-case DIPG Registry

- 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.

- Previously: eFLINT specification of DIPG regulatory document
- Today: Answer compliance questions using eFLINT specifications



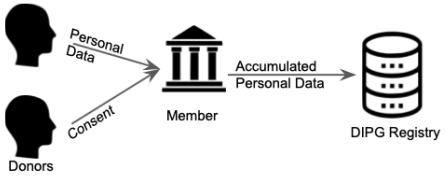
Dynamic generation of access control policies from social policies

1. Paper under submission for ICTH Conference
1. eFLINT is used to specify both higher level policies (GDPR, DSA) and lower level policies(access control policies).
2. Extensions to eFLINT make it possible to automate high level compliance decisions for example using access control

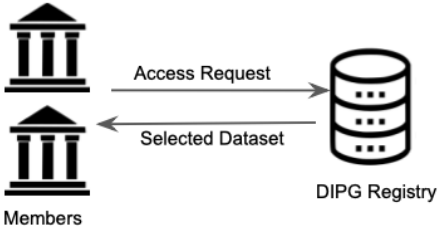
Compliance questions

According to the GDPR and the DIPG regulatory document:

1. What conditions need to be fulfilled by a member before making data available?



2. What conditions need to be fulfilled when accessing data from the registry?



Compliance Question 1

GDPR – Article 6(1)(a):

Personal data can be collected for a specific purpose if consent has been given for that purpose

GDPR – Article 5(1)(d):

Data must be accurate for purpose specified

```
1 Act collect-personal-data
2   Actor controller
3   Recipient subject
4   Related to data, processor, purpose
5   Conditioned by accurate-for-purpose(data, purpose), subject-of(subject,data)
6   Creates processes(processor, data, controller, purpose)
7   Holds when consent(subject, controller, purpose)
```

Compliance Question 1

DIPG Regulatory document – Article 4(2):

Members should transfer data to the DIPG registry in a coded form only

```
1 Fact coded Identified by dataset
2 Act make-data-available
3   Actor institution
4   Recipient  dcog
5   Related to  dataset
6   Conditioned by  coded(dataset) Holds when member(institution)
```

Compliance Question 1

```
1 Extend Act make-data-available Syncs with (Foreach donor:
2   collect-personal-data(controller = institution
3                         ,subject    = donor
4                         ,data       = dataset
5                         ,processor  = "DCOG"
6                         ,purpose    = "DIPGResearch")
7     When subject-of(donor, dataset))
```

An institution can make a dataset available when (for each donor (subject) in the dataset):

- The institution should be a member of the consortium
- Data should be coded
- Consent is given by the donor for the processing of their personal data by the DCOG for the purpose of DIPGResearch
- Data should be accurate for the purpose DIPGResearch

Compliance Question 2

```
1 Fact actor
2 Fact recipient
3 Fact asset
4 Act  access Actor actor Recipient recipient Related to asset
5 Act  read   Actor actor Recipient recipient Related to asset
6 Act  write  Actor actor Recipient recipient Related to asset
```

Read and write action are instances of access action (formalisation omitted)

```
1 Extend Act read Holds when (Exists project, institution:
2   selected(asset,project) && approved(project,institution) &&
      affiliated(actor, institution))
```

An actor can *read* an asset when (there exists a project and an institution for which):

- The asset is selected for the project
- The project is approved for the institution
- The actor is affiliated with the institution

More Examples

Granting read and write permission to dataset owners

```
1 Fact owner-of Identified by institution * dataset
2 Extend Act make-data-available Creates owner-of(institution, dataset)
3 Extend Act write Holds when affiliated(actor,institution)
4                          && owner-of(institution, asset)
5 Extend Act read  Holds when affiliated(actor,institution)
6                          && owner-of(institution, asset)
```

An actor can write or read an asset when:

- The actor is affiliated with an institution
- The institution is the owner of the asset

Conclusion

1. Answer compliance questions
   - Using eFLINT specifications
   - eFLINT is used to specify higher-level concepts (`collect-personal-data`) and lower-level concepts (`read` and `write`)
   - We introduced eFLINT extensions that enable us to connect higher-level and lower-level concepts : as demonstrated by the generation of access control rules
   - The approach in the paper is for a centralised solution
1. Future work
   - Develop a decentralised solution

Research output

1. Critical reflections on ODRL
   - AICOL International Workshops 2018-2020,AI Approaches to the complexity of Legal systems. LNAI Springer Series.
2. Position paper - Automating normative control for healthcare
   - AICOL International Workshops 2018-2020,AI Approaches to the complexity of Legal systems. LNAI Springer Series.
3. Dynamic generation of access control policies from social policies (Under submission)
   - ICTH 2021:The 11th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2021)

RQ5: Automating normative control for Healthcare research

Milen G. Kebede

Informatics Institute, University of Amsterdam
m.g.kebede@uva.nl

July 1, 2021