BATMAN

Privacy Design

General #1

- Data is separated in different “bags”, each bag requires certain permissions in order to be accessed.
    - Example of bags:
        - Personal information
        - Steps
        - DNK
        - Health Record of Type X
- There are 3 basic types of groups:
    - Patients
    - Medical Staff
    - Researchers

General #2

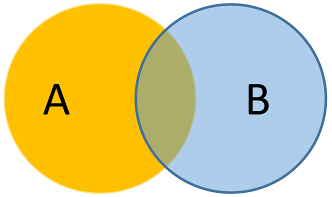
- There are 3 basic types of groups:
    - Patients
    - Medical Staff
    - Researchers
- Each group has a set of permissions
    - Example:
        - Medical staff can access user’s medical records, modify and add data
        - Researches can access anonymized medical reports of type X (e.g. steps)
        - Patients can see all their data, who can view their data

General #3

- Each group has a set of permissions
  - Example:
    - Medical staff can access user’s medical records, modify and add data
    - Researches can access anonymized medical reports of type X (e.g. steps)
    - Patients can see all their data, who can view their data
- User:
  - User belongs to one or more groups
    - Example: Doctor X belongs to group *Medical Staff from Ljubljana* and *Research group in Ljubljana*
  - The access to data depends on his groups permissions

Groups

- Groups have unique name -> Ljubljana
- Each group has 3 subtypes: patient, researcher, medical staff
- Each group can set individual permissions for subtypes
- User can be in multiple groups
  - If patient is in multiple groups, permissions are aggregated by intersection of groups



Patient Group	Researcher Group	Researcher Permissions
A	A	A
A	B	None
A, B	B	B
A,B	A,B	$A \cap B$

Use case example #1

- Users:
  - Janez [Ljubljana:patient]
  - Mirko [Ljubljana:medical]
  - Marko [Ljubljana:researcher]

- Scenario:
  - Janez fills in questionnaire about his lifestyle habits.
  - Mirko can view what Janez filled in
  - Marko can view statistics about questionnaire in Ljubljana e.g. how many patients answered questions, what their answers were etc. but he cannot connect patient X to questionnaire answer

Use case example #2

- Users:
  - Janez [Ljubljana:patient]
  - Jovani [Trst:patient]
  - Marko [Ljubljana:medical, Trst:researcher]

- Scenario:
  - Janez and Jovani fill in questionnaire about their lifestyle habits.
  - Marko can view:
    - What Janez answered, since he is his doctor
    - What some patient answered in Trst, because he is researcher in that group

Use case example #2

- Users:
  - Marko [researcher-Ljubljana, researcher-Trst]

- Scenario:
  - Marko is in two groups, he can view the researcher based data from the groups.