This is a list of use cases supported by this specification. These use cases will be further detailed.

### Patient Privacy considerations and requirements (WIP)

Access to read or change FHIR resources, or elements, or a set of elements, must depend on a set of rules and criteria (Requirement 1). Therefore, the actors (patients themselves, regulators, or practitioners) must have their access based on those rules, and must be able to consult those rules (Requirement 2). These access rules are managed by other actors, and access to these access rules is itself depending on the rules defined by the actors.

There are different justifications for data exchange, namely those in GDPR. When addressing health data, which is sensitive information, special safeguards are to be put in place, and the consent by the patient has to be considered in the context – in a context of care, patients are usually not in a position to give explicit, specific and free consent.

#### Story map

##### R01

Different access permissions to data:

1. Patient roles can access their demographics and personal data

* Setting of simple access rules
* Grant access to certain roles
* Remove access to any role\*
* Evaluate impact of my consented access

1. Patients roles have access to clinical data (e.g. AllergyIntolerance)
   1. Rules apply to different resource types, as determined by the roles and purposes – must distinguish between primary and secondary data.
2. Rules should be dependent on profile or transaction, because the same resource (e.g. CarePlan, Observations) can be used in different contexts with different sensitivity constraints
3. Patients can grant access for specific purposes only
4. GPs can see the access the data but of patients only if they are their family doctors
   1. Access control must be extended to sub-roles and relations
5. As care giver I cannot access the NISS number of the patient, only the name
   1. Access to some fields may be restricted
6. As a care giver I cannot access patient health data marked as “private”
   1. Need to classify the data elements, sets of elements, or resources
7. As a care giver I can search for data, but I cannot obtain data that is beyond my access level
   1. Not allowed:
      1. AllergyIntolerance?subject.address=Privéstraat
      2. AllergyIntolerance?subject.SSIN=123456789
   2. Allowed
      1. /AllergyIntolerance?code=Hay fever
      2. /AllergyIntolerance?subject.family=Janssens

##### R02

Access to system and access managers:

1. Access managers can see the content of the Personal Data Access Rules
2. Some rules are enabled but not visible to the patient - e.g. if the law requires some data to be shared with or without consent, the patient may not see that.
   1. Example cases:
      1. Mandatory reporting of infectious diseases
      2. Court-ordered access to data
3. Patients can see the content of the personal data access rules (the rules that they are allowed to see)
4. Patients can see which individuals (not only roles) has access to their data
5. Patients can refuse consent to data by some users (note that refusing consent is not the same as blocking access)
6. Access managers’ access to the Personal Data Access Rules is itself limited by a set of rules (Access Control Rules)
7. Any change of access (from the any of the actors) must be checked for errors – if a user tries to change a rule outside their permissions, or a conflicting rule, this will be logged
8. Users and access managers must have a User Interface to monitor their permissions (in the scope of their visibility to them)