In the health domain, it is imperative to both protect personal privacy, and enable sharing of data to better treat individuals. Currently, data sharing and protection policies are created and enforced by the hospitals and institutions that collect and store this information. However, these centralized, from-the-top-down policies may not reflect an individual’s personal sharing and privacy beliefs. For instance, an individual may believe that sharing all, and unanonymized, information for research purposes far outweighs the privacy invasion. It is essential that individuals can clearly express what they wish to provide access to at a fine-grained level. Tools such as MyKinMatters, Figure 1, allow individuals to identify health-resources, and share them with family members.

Moreover, within the medical domain, some information is not owned by an individual. For instance, genetic information that is carried within a family is not an individual’s data, but familial data. It is about, owned, and impacts a group. The specific test results about a genetic-based disease’s expression in an individual is owned by that individual, but the underlying genetic information is familial.

Thus, if we try to enable personalized statements of data access, when resources are owned by set of people and they all have different preferences regarding how the resources should be accessed. This project explored how to effectively state and reason over the data access requirements for multiple holders of the same data. In order to this, many use cases of families and genetic diseases were compiled. From there, a policy language was created that allows individuals to clearly express who each resource should or should not be shared with. An example of an entry in this policy language is shown in Figure 2. This language was used to describe the access requirements in all of the use cases.

Once individualized access requirements are expressed, it is possible to reason over them automatically to detect the conflicts of data sharing wishes for a given resource.

Moving forward, the policy language will be compared to other privacy policy languages such as P3P and XACML to determine how it compares to those languages with respect to expressiveness. Additionally, the policy language will be mapped to other efforts, such as Personalized Consent, that use conjunctive queries (CQ) to allow users to express their preferences.
Figure 1: MyKinMatters. A tool to help patients organize their genetic information and share with appropriate family members.

```java
author Sam
resource[Y]{
  share
    + Children():
    + aunts():
    - uncle():
  never
    maternalUncle("mike"): {
    }

author Sam’s Mom
resource[Y]{
  share
    + grandSons(): age > 15
  never
    daughter("Maria"): -> [parent():]
  }

author clinician
resource[Y]{
  share
    get(SamID).firstDegree():
    get(SamID).secondDegree():
  }
```

Figure 2: Example policy from two individuals for the same medical resource, describing access to the data.