Individuals desire the ability to gather, share, and control their health data. (Give Me My DaM Data!) Currently, health data can be found on paper, digitally in databases, spreadsheets, software (such as electronic medical records), in various devices, apps, or clouds, and people’s memories. The sources of this data is often spread far and wide and may be impossible or arduous to find. The older the person and the more complex the illness challenges, the more likely that the data is in a growing number of places. Also, the more complex the illness challenges the more likely that individual or their care partner is the vehicle of sharing that data. Some people want to know and give permission to who has access to or is accessing that data. They may change their minds about this over time. Many people entrust a family member / care partner to manage their data for them.

Clinicians, other health professionals, community health workers, researchers, healthcare organizations, policy makers, and insurers want or need health data to diagnose, plan care, pay for care, create evidence of practice and treatment effectiveness, and communicate with individuals receiving care and each other.

Adding to the difficulty is the sheer volume of data, sometimes the lack of data, and the inevitable errors in data – like drinking dirty water from a firehose.

Necessary to this data exchange are standards for data elements, data security, permissions, and data correction. The data means the same thing wherever it’s housed. It requires trusting relationships in dangerous waters - trust between people, organizations, vendors, and government in any combination. It won’t happen by itself. It requires a team devoted to collaboration - finding, proposing, testing, and communicating solutions. Standards already exist. They’re called HL7, FHIR, OAuth, OpenID CONNECT, UMA and more. These standards fill different needs and need to work together. If they contradict each other it’s just more mess. To add insult to injury this crazy complicated problem needs a simple solution, so everyone can understand it and use it. To keep this process honest and grounded in real people’s experience, it helps to picture different users of data using it in different ways with different needs and desires. These are called *use* cases.

*The HEART Working Group intends to harmonize and develop a set of privacy and security specifications that enable an individual to control the authorization of access to RESTful health-related data sharing APIs, and to facilitate the development of interoperable implementations of these specifications by others*