Personal data safety for refugees on the move: securepod

FAIR stands for **Findable**, **Accessible**, **Interoperable** and **Reusable**. By making data FAIR, data reuse is improved, by ensuring that one can easily find and access data, and that the data is interoperoperable so that it is usable in different places and systems.

Data ownership is especially crucial for vulnerable groups such as refugees, whose personal and medical data is often split up between countries and thereby usually inaccessible. They face heightened risks regarding the security of their personal data due to factors such as displacement, overlapping legal frameworks, and the need to share information with various entities. The concept of personal datapods has been presented as a solution to some of these issues, allowing refugees to own and store their data. The FAIR data principles are embedded into the core design of these datapods. This approach not only strengthens the protection of personal information but also ensures secure and efficient access when needed.

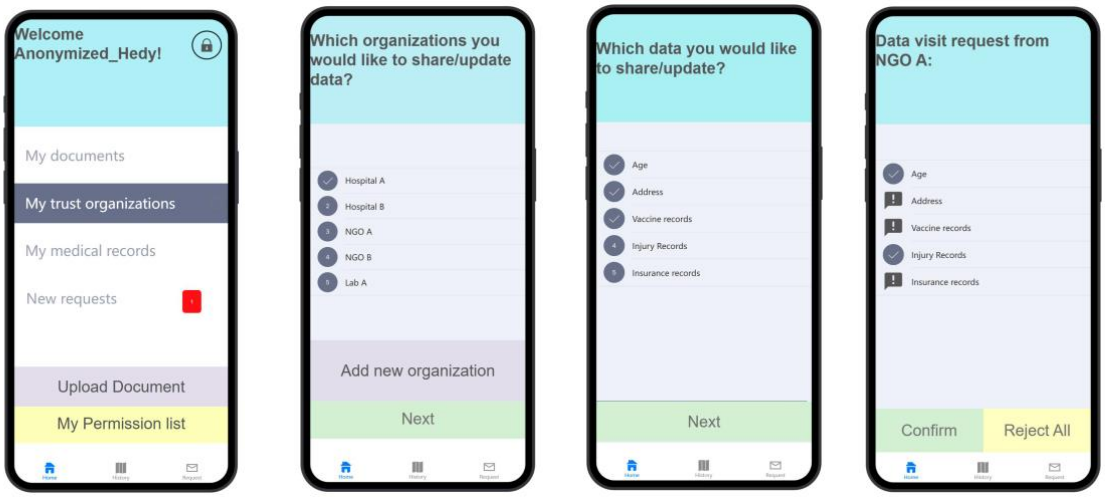

Figure 1. Example of what the securepods would look like on a phone.

The pods allow refugee to update their data and manage official documents. It also enables them to selectively grant and revoke access to their data. The data that is uploaded is done so in a FAIR format, ensuring interoperability.

RECOMMENDATIONS

1. Establish interoperability guidelines that ensure refugee data stored in datapods can be seamlessly shared across borders and between different agencies or governments, while adhering to FAIR data principles (Findable, Accessible, Interoperable, and Reusable). These guidelines should also align with international humanitarian data standards.
2. Establish policies that promote data portability, ensuring that refugees can continue to access and manage their personal datapods even when they move across borders or change regions. This should include cross-jurisdictional agreements to allow secure data portability between countries and agencies.
3. Develop transparent data-sharing agreements between governments, humanitarian organizations, and other stakeholders. These agreements should explicitly outline the conditions under which refugee data can be accessed or shared and should include audit mechanisms to ensure compliance.
4. Develop digital literacy programs to educate refugees on managing their data through datapods and understanding their data rights. This should include guidance on how to safely share, update, or revoke access to their information.
5. Establish crisis-responsive data management systems that can adapt to emergency situations, such as natural disasters or political crises, ensuring continued access to refugee datapods and secure backup systems to prevent data loss.