In the current model of data sharing between vulnerable community members and nonprofits, community members give their personal information to nonprofits to receive services in a transactional arrangement and after they give their data they don’t know how it is used, stored or protected.

Community organizations are willing to be transparent but struggle to do so because of logistical, technical, and fiscal barriers. Data management solutions provide software to nonprofits and are uniquely positioned to facilitate the relationship between nonprofits and community members.

A Data Collection Handbook: Six Principles for a Privacy Preserving Framework for Data Collection

- Six core principles to guide designs
- Definitions for each principle
- Findings from our research
- Guidelines for improving each principle
- 25 solution examples
- 6 solution visualizations

Comfort
The community member’s willingness to give their data with ease and without hesitations and with confidence that their data is handled correctly.

Trust
The community member’s confidence that the organization they are giving their data to has their best interest at heart and is being honest and fair.

Communication
Any exchange of information between the organization and the community member, both directly and indirectly, like websites or flyers.

Security
The confidence a community member feels that their data is being appropriately stored and protected.

Ownership
Ownership is the control or agency the community member has over any data they give, even after it is given.

Value
Value is a fair return to the community member by the nonprofit in exchange for the provision of their data.

86% of respondents participated in community programs.

“They fear that what they say might impact the services they receive.”

“You just accept without even thinking about it.”

“Everyone should have the option to decide how their information is used.”

“Comfort depends on the reason. It has to be a clear and good reason.”