**Requirement:**

Projects collecting data must identify the types of data collected and stored. Projects must also demonstrate how they ensure the privacy and security of this data in addition to the steps taken to prevent adverse impacts resulting from its collection, storage, and distribution.

**Approach taken for development of Aajeevika:**

The Entity Relationship diagram defines the various data types for the data collected in the application.

We are collecting the master data from the government regarding the schemes, products, locations, CLFs, collection center etc. and storing it in the database either via bulk upload or through the web screen. This is done via authorised users only. The transaction related data is uploaded by the sellers and the buyers who are the registered users of the system.

The application vulnerabilities are handled through Open Web Application Security Project (OWASP) application security verification standards. In order to make the application secure, the following security risks are being taken care of:

* Broken Access Control
* SQL Injection
* Insecure Design
* Security Misconfiguration
* Cross-Site scripting

UNDP has done User Acceptance Testing for the application.