# *Guidance Document for the Protection of Human Subjects' Identities*

This guidance document is designed to meet the standards as set in the *UNICEF Procedure for Ethical Standards in Research, Evaluation, Data Collection and Analysis*. It is designed to ensure effective processes and accountability for ethical oversight of these processes; to ensure the protection of, and respect for, human and child rights within all research, evaluation, and data collection processes undertaken or commissioned by UNICEF.*

Providing subject *anonymity* means that either the project does not collect identifying information of individual subjects (e.g., name, address, email address, etc.), or the project cannot link individual responses with participants' identities If it is essential to collect and link identifying information to subjects' responses (e.g., questionnaire answers), researchers must do their best and may need to be creative to provide the utmost *confidentiality* of subject data.

Maintaining confidentiality of information collected from research participants means that only the investigator(s) or individuals collecting/analyzing data can identify the responses of individual subjects. However, researchers must make every effort to prevent anyone outside of the project from connecting individual subjects with their responses.

The following are examples of practices that may be implemented to increase the level of confidentiality:

- Use a unique subject code on data documents (e.g., completed questionnaire) instead of recording identifying information. Keep a separate document that links the code to subjects' identifying information locked in a separate location and restrict access to this document (e.g., only allowing primary investigators access).
- Encrypt identifiable data.
- Remove face sheets containing identifiers (e.g., names and addresses) from survey instruments containing data after receiving from study participants.
- Thoroughly dispose, destroy, or delete study data and documents in accordance with pre-determined timeframes for storage and inquiries.
- Have clear guidelines on how data is transported or transferred (i.e., encrypt if electronic, prohibit staff taking data home to work on or ensure that if data is moved that the storage device (e.g., USB/hard drive) is password protected.
- Limit those who have access to identifiable information.
- Securely store data documents within locked locations.
- Assign security codes to computerized records.

*See: *UNICEF Procedure for Ethical Standards in Research, Evaluation, Data Collection, and Analysis*; Document Number: CF/PD/DRP/2015-001 Effective Date: 01 April 2015 Issued by: Director, Division of Data, Research, and Policy (DRP).