Guidance Document for Protection of Research Data

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.*

Data protection should be a part of every project's plan for data storage. Confidentiality and anonymity can be assured by replacing names and other information with encoded identifiers, with the encoding key kept in a different secure location. To maintain its integrity, whether in written or electronic form, project data should be protected from tampering, loss, theft, or physical damage by limiting access to data. Principal Investigators should decide which project members are authorized to access and manage stored data. Data stored on paper, such as surveys or notebooks should be kept together in a safe, secure location away from public access.

Electronic data storage offers many benefits but requires additional consideration and safeguards. Theft and hacking are concerns with electronic data. Electronic data can be protected by taking the following precautions:

- use unique user IDs and passwords that cannot be easily guessed;
- change passwords often to ensure that only current project members can access data;
- provide access to data files through a centralized process;
- evaluate and limit administrator access rights;
- ensure that outside wireless devices cannot access your system's network;
- keep updated anti-virus protection on every computer;
- maintain up-to-date versions of all software and media storage devices;
- use a firewall and intrusion detection software to monitor access for internet connected storage;
- use encryption, electronic signatures, or watermarking to keep track of authorship and changes made to data files;
- regularly back up electronic data files (both on and offsite) and create protected copies;
- ensure that data are properly destroyed.

There is no set amount of time that should be stored and may be at the discretion of the PI. However, many sponsor institutions require that data be retained for a minimum number of years after the study's completion. HML IRB suggests that project data be retained for three years after the study ends. Other sponsors or funders may require longer or shorter periods.

*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).

HML Institutional Review Board
www.hmlirb.com   Washington, DC USA   unicef@hmlirb.com