Data Protection Plan Requirements and Guidelines for Obtaining PSID Restricted Data

This document describes the required contents of the Data Protection Plan that must be submitted as part of the application for PSID restricted data. It describes the basic information that all Data Protection Plans should include, the type of protection expected, and the disclosure rules for presenting and publishing results on these data.

The Data Protection Plan must describe the following elements of the work and computing environments.

1. Types of Protection Expected

Below are the data protection requirements for PSID restricted data. Your data protection plan should describe how your work environment will protect the data, for each of these features or their equivalent:

- Standalone, non-networked PC or authorized data enclave
- No use of the data on laptop computers
- Data may be used only by individuals with contractual authorization for data use
- Data use must be in office environment described in security plan and not at home or any other off-site location
- Password-protected access to all computers storing the data
- Automatic activation of password-protection after five minutes of inactivity on the computer
- Encryption with password protection of all files containing data (identify encryption software to be used)
- No automated backup copying of the data
- Secure storage of any and all removable devices holding the data (e.g., CDs, diskettes, zip drive disks, etc.) through encryption and storage in a locked compartment or room when not in use
- Storage of detailed printouts derived from data analysis in a locked compartment or room when not in use
- Shred all detailed listings and printouts that are no longer needed
- Prepare and maintain a log of all data files acquired. Record dates that data and paperwork are received and returned or destroyed
- Pledge to destroy or return all files containing Restricted Data at the end of the project
- Report any and all violations of the Data Safeguarding Plan to PSID, the Restricted Data Investigator, and the home-institution IRB
- No transmittal of data or detailed tabulations with cell sizes of less than 11 via e-mail or e-mail attachment or FTP (either over the Internet, an Intranet system, or within a local area network).
- Brief all research staff that have access to the Restricted Data about the Data Protection Plan, appropriate data use, and penalties for inappropriate use.

The Restricted Data Investigator must regularly monitor procedures for use of the data by all project staff and collaborators. Clear rules about Restricted Data use should be posted in a location that is readily visible to staff. At the conclusion of the research project, all the original Restricted Data media must be destroyed or returned to PSID and all data files and unpublished printouts must be destroyed.

2. Disclosure Rules

The Data Protection Plan must carefully describe how researchers and staff members will avoid inadvertent disclosure of respondents' geographic locations or identity in all working papers, publications, and presentations.

At minimum, researchers must agree to exclude from any type of publication or presentation, the following information:

- Listing of individual cases;
- Description of individual cases;
- Listing, description, or identification of a tract or tracts by number, by name, or by descriptive information;
- Maps with any features (such as landmarks, road networks, original tract shape or physical features) that allow tracts to be identified; and
- Summary statistics or tabulations that have cell sizes under 11 observations.

Data Protection Plan Description:

1. List and describe all locations where the original and any copies of the data will be kept (and provide building name, street address, and room numbers);
2. List names and include CVs of all individuals who will be accessing the data;
3. Describe the computing environment in which the data will be used, including:
    - Computing platform (e.g., personal computer, workstation, mainframe) and operating system;
    - Number of computers on which data will be stored or analyzed;
    - Confirm that PCs used in the research project will be stand-alone.
    - Physical environment and address in which computer and data are kept (e.g., in room with public access, in room locked when not in use by research staff);
    - A list and description of all devices on which data will be stored (e.g., mainframe computer storage device, PC hard drive, removable storage device such as CD, floppy drive, or zip drive);
    - Methods of data storage when data are not being used;
    - Methods of transmitting the data and results between research team members (if applicable);
    - Methods of storage of computer output both in electronic form and in hard copy (on paper or other media); and
    - Instruction in data protection policies that will be provided to each staff member and student before they receive access to the data as well as recurrent instruction that will be conducted at least annually.