



## Form #4 II. Developing a Data Protection Plan

Sealy Center on Aging, University of Texas Medical Branch

301 University Blvd. Galveston, TX 77555-0177

### 1. Restricted Data Plan Standards

Investigators that request to obtain MHAS restricted data must submit a Restricted Data Protection Plan for approval by the MHAS staff. The Restricted Data Protection Plan is part of the wide effort to maintain the anonymity of respondents and that only authorized persons in the contract have access to the contents of MHAS restricted data. The following should be considered when drafting the Restricted Data Protection Plan:

**Restricted Data:** Any data from the Mexican Health and Aging Study that might compromise the anonymity or privacy of respondents to that study, or which has been obtained from an agency that requires restrictions on the release of the data. This includes any data file for individuals, families, households, employers, or pension or other benefit providers, that contains any of the following items:

- a. Geographic identification of areas smaller than Census Division, including, but not limited to, metro area, county, minor civil division, school district, city, place, zip code, tract, block numbering area, enumeration district, block group, or block
- b. Social Security Covered Earnings Data
- c. Wage and Self-Employment Income data
- d. Social Security Retirement, Survivors and Disability Insurance (RSDI), Supplemental Security Income (SSI/SSDI), and Form 831 Disability data
- e. Occupation data
- f. Pension Provider data
- g. Exact date (month, day, and year) of interview or of birth/death of respondents or family members
- h. Any variables or fields derived from the data mentioned in items a. through h., including data linked to a MHAS dataset using data from items a. through h.

**Authorized Person:** A Restricted Data Investigator, Co-Investigators, Research Staff, and network/system administration personnel who have signed the restricted data agreement.

**Removable Media:** A storage device that can be removed while a computer is powered on and includes compact disks (CD ROM, DVD, and Blu-Ray), diskettes, USB/Firewire drives, memory cards, media player devices, smartphones, digital cameras, Bluetooth devices,

magnetic tapes, punch cards, and/or any other electromagnetic, optical, or paper storage device.

## 2. Required Restricted Data Protection Plan Components

- Data Protection Plan Narrative
- A copy of the Restricted Data Order Form specifying requested data sets
- A copy of the Restricted Data Protection Plan Checklist

### A. Data Protection Plan Narrative

The narrative must address each of the following topics.

i. **Overview:** The data protection plan should describe the computing environment in which the data will be stored, managed and analyzed. Such information will provide the necessary background information to MHAS staff to determine how secure the computing environment may be.

ii. **Shared File System:** Whether a shared file system will be used to store MHAS restricted data will need to be stated in the Restricted Data Protection Plan. The following information in this sub-section **only** applies if authorized users will use a shared file system

If you will be using a shared file system to store MHAS restricted data, such as a Local Area Network (LAN) or a timesharing mainframe, describe the system architecture as a whole, including connectivity between servers and your desktop client, intrusion detection/prevention methodology, location of network storage devices, and methods used to protect network components from unauthorized access. Describe the procedures that will be used to prevent network access by unauthorized persons to files containing MHAS restricted data. Include information on access rights, password assignment and management of file ownership. You should also specify how data in transit between client and server will be protected (e.g., VPN protocols, VLAN technology). Finally, describe how you will prevent routine network and system backups of storage device files containing restricted data, regardless of whether such backup copies are on magnetic tape, hard disk, diskettes, or otherwise.

iii. **Workstation Storage:** Whether a local storage device will be used to store MHAS restricted data will need to be stated in the Restricted Data Protection Plan. The following information in this sub-section **only** applies if authorized users will use a local storage device.

If you intend to use a local storage device (hard drive or other electronic or optical fixed device) to store MHAS restricted data, provide a description of how you will protect the

workstation from unauthorized physical and electronic access. Include a discussion of how your encryption software, anti-virus and anti-spyware software, password protection settings, firewall and physical protection methods will interact to produce a secure environment. Describe how the operating system will be configured to limit access to HRS restricted data local storage devices; e.g., read/write permission settings, authentication protocols, and folder or whole-disk encryption.

iv. **Use of Removable Media:** It is recommended not to use removable media for storage of Restricted Data.

Whether removable media storage will be used for MHAS restricted data will need to be stated in the Restricted Data Protection Plan. The following information in this sub-section **only** applies if authorized users will use removable media.

If you will be using removable media storage for restricted data, your plan must state where the removable media to be used will be physically located and how physical access to them is to be restricted, including provisions for storage in locked cabinets when not in use. Your Plan should also specify how access to the contents of removable storage device files containing MHAS restricted data will be controlled, for example, through use of encryption and password protection.

Some computing systems employ centralized handling of removable media (such as magnetic tapes used for backups) requiring the use of keywords or labels (internal and/or external), known only to the owner of the removable medium, to mount the medium. Other systems allow the owner to specify which other users can have read/write access to a removable storage device. Your Plan should state how mechanisms of this sort will be used to ensure that only authorized persons will be able to mount and read removable media handled by a central system.

v. **Backups:** For archival purposes you may make one backup copy of each removable media item containing MHAS restricted data. If you intend to create such archival backups, your Plan should state that you will make only one backup copy of each item received from MHAS. Removable media items sent to you by MHAS should be stored in the same secure fashion as archival backups. The Plan should describe the physical and/or software methods what will be used to protect distribution and backup media from unauthorized access.

Note: At the termination of your agreement, on or before the date on which your authorized access to the data expires, all distribution, work-space, and archival backup copies of MHAS restricted data must either be returned to MHAS or destroyed (written over or otherwise made unreadable). If you choose to destroy the data, you must provide a counter-signed statement confirming the destruction of the restricted files.

vi. **Paper Printouts:** Describe how you will restrict access to paper printouts containing information derived from MHAS restricted data. The MHAS staff strongly recommends against the creation of any paper printouts containing restricted data, and will be very skeptical of any Restricted Data Protection Plan that proposes the use of such printouts.

If you will not be using such printouts, state this in your Restricted Data Protection Plan and disregard the rest of this sub-section.

If you will be using paper printouts containing restricted data, your Plan must clearly state the uses that will be made of such printouts and the reason(s) why no other media can be used for the same purpose. Your Plan must also specify the means by which you will ensure that such printouts cannot be accessed by unauthorized persons (e.g., kept in locked storage that is accessible only to authorized persons when not in use); how they will be shielded from the vision and reach of unauthorized persons when they are in use; and how they will be destroyed (made unreadable, e.g., through shredding) prior to the termination of the restricted data agreement.

vii. **Treatment of data derived from restricted data:** MHAS requires a clear statement that you will treat all data derived from restricted data in the same manner as the original restricted data, and that you understand that data derived from restricted data includes, but is not limited to:

- a. Subsets of cases or variables from the original restricted data;
- b. Numerical or other transformations of one or more variables from the original restricted data, including sums, means, logarithms, or products of formulas;
- c. Variables linked to another dataset using variables from a MHAS restricted dataset as linkage variables.

(Aggregate statistical summaries of data and analyses, such as tables and regression coefficients, are not "derived variables" in the sense used in the Agreement, and are not subject to the requirements of the Restricted Data Protection Plan and the Agreement as long as cell size limits are observed.)

viii. **Linkages to other datasets:** State which other MHAS and non-MHAS datasets, if any, you intend to link to the MHAS restricted data you are requesting, and a clear statement that you will not perform linkages to any other datasets. Your statement must include recognition of the following rule:

- a. No MHAS restricted dataset may be linked to any other MHAS restricted dataset without the explicit written permission of MHAS

**B. Restricted Data Order Form:**

Since your Data Protection Plan needs to match the MHAS restricted data set(s) you are requesting, it should be included as part of your application package. Note: Specify the file format/encryption type for each product that you request.

**C. Restricted Data Protection Plan Checklist:**

The checklist provides MHAS with an overview of the computing environment in which your research will be conducted. It will be used in conjunction with the documents described above to determine if your application can be approved by the Data Confidentiality Committee. This document must be signed by you and an IT department representative.

If your computing environment does not match the checklist requirements, you must include a document that provides justification for each difference. Areas of special concern are:

- Workstation operating systems not on the checklist.
- Workstation access by multiple users.
- Missing anti-virus and anti-spyware software.
- Encryption software and how it is handled at the server and workstation.
- How physical access to computing equipment (client and server) is controlled.
- Encryption of network traffic between client and server (if applicable).
- Network server access procedures (if applicable).
- Implementation of firewall and intrusion detection systems (if applicable).