Elements of a Successful HRS Data Security Plan

Overview

Your data security plan (DSP) should provide a general description of the computing environment in which you will manage and analyze the data. This overview provides guidance on how to ensure data security. Please be sure to note in your DSP how you address each recommended action.

Shared File System

If you will **not** be using a shared file system to store HRS restricted data, state this in your DSP. This is preferred by HRS.

If you **will be using** will a shared file system with HRS restricted data, 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 HRS 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 HRS restricted data.

Workstation Storage

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

Storage of Removable Media Items sent by HRS

The removable media devices sent to you by HRS containing restricted data must kept in locked storage that is accessible only to authorized persons when not in use. Indicate this in your DSP. HRS strongly recommends against the use of removable media for storage of restricted rata, with the exception of one copy for back-up (see below).

Backups

For archiving, you may make **one** removable backup copy of HRS restricted data. If you intend to create such archival backups, your DSP should state that you will make only one backup copy of each item received from HRS. Backup archival copies should be stored in the same secure fashion as originals sent to you by HRS. No cloud-based back-up is allowed.

Return or Destroy at Termination

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 HRS restricted data must either be **returned to HRS or destroyed**. If you choose to destroy the data, you must provide a counter-signed statement confirming the destruction of the restricted files and how you destroyed them.

Paper Printouts

If you **will not** be using such printouts, state this in your DSP and disregard the rest of this sub-section.

If **you will be** using paper printouts containing restricted data, your DSP 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 DSP 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.

Treatment of data derived from restricted data

We require 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 an HRS restricted dataset as linkage variables.

Aggregate statistical summaries of data and analyses, such as tables and regression coefficients, are not considered derived variables and are not subject to the requirements of the DSP and the Agreement as long as cell size limits (n>=5) are observed.

For additional guidance on reporting analysis results of HRS restricted data, please review Maintaining Respondent Privacy and Anonymity: Guidelines for HRS Restricted Data Users on this Web site.

Linkages to other datasets

State which other HRS and non-HRS datasets, if any, you intend to link to the HRS 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 rules:

a. No HRS restricted dataset may be linked to any other HRS restricted dataset without the explicit written permission of HRS;
b. No dataset including geography at a level of detail finer than Census Division (including the HRS Wave I Interview Dataset) may be linked to any restricted data product derived from Social Security administrative records.