GUIDANCE FOR PREPARING AN SSA DATA PROTECTION PLAN

Introduction

As a potential user of SSA sensitive data, you must submit a **SSA Data Protection Plan for each facility (site) where SSA sensitive data is maintained** to the Office of Research, Evaluation, and Statistics (ORES) for approval. You must specify in your **SSA Data Protection Plan(s)** how you will keep SSA data secure and confidential on a variety of media, including magnetic tapes, hard disks and other fixed magneto-optical media; compact disks, diskettes, and other removable magneto-optical media; and paper. Use the following **Guidance for Preparing an SSA Data Protection Plan** to write your **SSA Data Protection Plan**. Describe in detail each provision listed (**use additional paper (8 ½ x 11) if needed**).

The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III – Security of Federal Automated Information Systems (http://www.whitehouse.gov/omb/circulars/a130/a130.html) which sets forth guidelines for security plans for automated information systems in Federal agencies.

SSA Sensitive Data

SSA sensitive data includes any data from SSA's administrative records that might compromise the anonymity or privacy of individuals. It also includes any variables or fields derived from our administrative records, including linked or matched variables. The major sources of SSA administrative data are, but are not limited to, the following systems of records:

- **Master Beneficiary Record (MBR) –** Payment file from which Social Security checks are paid. The MBR contains information on Title II beneficiaries, such as payment status, type and amount;

- **Supplemental Security Record (SSR) –** Payment file from which Social Security Income (SSI) checks are paid. The SSR contains information on Title XVI beneficiaries, such as payment status, type and amount;

- **831 Disability File –** This file contains medical determinations made by the Disability Determination Services (DDS) for Social Security and SSI claims;

- **Completed Determination Record** (also known as the Disability Control File or DCF) – This file contains information on allowed disability claimants (both Title II and Title XVI) on which a continuing disability review has occurred and a decision of continuance or cessation has been approved;

- **NUMIDENT –** Master file of assigned Social Security Numbers (SSNs). This file contains identifying information given by the applicant for an SSN and most of the vital status data that SSA provides health researchers through its **epidemiological service**, including state of residence and date of death; and

- **Master Earnings File (MEF) –** This file contains workers' earnings records and information on the individual's entire work experience.

GUIDANCE FOR PREPARING AN SSA DATA PROTECTION PLAN continued

Your SSA Data Protection Plan must include:

1. **Security/Physical Safeguards of the Computing Environment.**

   We strongly recommend that you use a self-contained Local Area Network (LAN) or a stand-alone computer (s) because of the potential security problems that can occur in timesharing mainframes or LANs. If you do use a timesharing platform, be very specific in describing the security and safeguards that you will use to protect our data.

   Provide a detailed description of the security/physical safeguards of the computing environment in which you will be managing and analyzing the data. For each item of the computing equipment you will be using (CPU, tape drives, printers, etc.), describe:

   a) Where they are located;
   b) Who has physical access to them;
   c) The security provisions that restrict access to only authorized users of the data on the system (s) you will be using, such as locked doors, locks on equipment, passwords, encryption, etc.;
   d) The routine procedures for making backup copies of data files on tape or disk;
   e) The system as a whole as well as your terminal;
   f) The access system administrators have to files and passwords [**For shared file systems only**];
   g) The audit trails which you maintain to identify users, authenticate users, and trace users' actions on your system. This enables you to maintain individual accountability of all data users.

2. **Restricted Access--Fixed Storage Media.** Provide a detailed description of how you will restrict access (e.g. password protection) to hard disk or other electromagnetic, optical or similar fixed storage device files containing the data. Indicate the kind of storage data you will be using and describe:

   a) Where the storage devices to be used are physically located;
   b) How you will restrict physical access to only authorized persons;
   c) How you will restrict access to the contents of hard disk and similar storage device files to only authorized persons, such as through a system of encryption and/or passwords;
   d) How you will restrict access to files to which only authorized users have "read" and "write" permission;
   e) How you will prevent routine system backups of hard disk and similar storage device files, regardless of type of backup medium;
   f) How you will prevent access to files by system administrators [**For shared file systems only**];
   g) Clearly in your Plan that no more than one backup copy will be made of any hard disk or similar storage device file containing the data;
   h) When (on or before the date on which your authorized access to the data expires) and how all such copies will be destroyed.

3. **Restricted Access--Removable Storage Media.** Provide a detailed description of how you will restrict access to compact disks, diskettes, and other removable electromagnetic or optical storage media files. We strongly recommend against the use of removable media for data storage, except as a means of shipping data to and from SSA. If used, describe:

   a) How you will use removable media data storage;
   b) Where the removable media to be used will be physically located;
   c) How physical access to them is to be restricted to only authorized persons, including provisions for storage in locked cabinets when not in use;
   d) Which mechanisms will be used to ensure that only authorized persons will be able to mount and read removable media; and
   e) Which mechanisms (e.g. computing systems that require the use of keywords or labels known only to the owner of the removable medium, to mount the medium) will be used to ensure that only authorized persons will be able to mount and read removable media handled by a central system [**For shared file systems only**].

4. **Printed Output.** Provide a detailed description of how you will restrict access to paper printouts containing SSA data. SSA strongly recommends against the creation of any paper printouts of its data. If used, describe:

   a) The uses that will be made of such printouts;
   b) The reasons why no other media can be used for the same purpose;
   c) The means by which you will ensure that such printouts are handled by authorized persons only;
   d) How they will be kept in locked storage, accessible only to authorized persons when not in use;
   e) How they will be kept from the vision and reach of unauthorized persons when they are in use; and
   f) How they will be destroyed (e.g. made unreadable through burning or shredding) after completing any analysis.

5. **Derivations of SSA Data.** Provide a clear and detailed statement that you will treat all derived SSA data in the same manner as the original SSA data, and that you understand that derived SSA data includes, but is not limited to:

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

   NOTE: Aggregated statistical summaries and analyses of the original data, such as tables and regression formulas, are not “derived variables” and, unless otherwise specified in the MOA, are not subject to the requirements of your plan.

6. **Linkages to Other Data.** Provide a clear and detailed statement that you will not link any other data to the original data specified in the MOA. Your statement must also include recognition that you will not link the original data or derived dataset (s) to any other SSA dataset(s) without our explicit written permission.

7. **Training for Individuals Who Will Have Access to Confidential Data.** All individuals who will have access to SSA data in identifiable form must understand the security and safeguard provisions required to assure the confidentiality of SSA data. Explain how you will train these individuals so they are familiar with the safeguarding provisions in your data protection plan. In addition, they will be required to sign a Confidentiality Statement (Attachment B).

Explanatory Notes

Authorized Persons. Authorized persons include the Custodian(s), the Principal Investigator(s), and any other persons or data users designated in the Memorandum of Agreement (MOA) and support documentation.

SSA Sensitive Data. SSA sensitive data contains identifiable personal information and information meant to be kept confidential as covered under SSA Regulation No. 1, the Privacy Act of 1974, the Tax Reform Act of 1976, and Section 1106 of the Social Security Act of 1974.

Title II. Provision of the Social Security Act. Title II is an insurance program. It was enacted in 1935 to provide old age, survivor, and disability benefits to insured individuals irrespective of financial need. [See 42 U.S.C. Sections 403, 423 (1982 ed. and Supp. III).]

Title XVI. Provision of the Social Security Act. Title XVI is a welfare program. It was enacted in 1972 to provide Social Security Income (SSI) benefits to financially needy individuals who are aged, blind, or disabled regardless of their insured status. [See 42 U.S.C. Sections 1382(a) (1982 ed. and Supp. III).]

Encrypted SSA Data. Where encryption is needed, encrypt SSA data using the Digital Encryption Standard, the only data encryption standard approved by the National Institute of Standards and Technology (NIST) for use by Federal agencies at this time.

Faxing SSA Data. We prefer that you not fax SSA data. However, if you do fax SSA data, documents must be properly labeled and the fax telephone number must be verified and an authorized person must be at the fax machine prior to sending the document.

Emailing SSA Data. We prefer that you not e-mail SSA data. However, if you do e-mail SSA data, it must be encrypted as an attachment to the mail message and sent to an authorized person only.

Protected Communications. We prefer that you not electronically transmit SSA data. However, if you do electronically transmit SSA data over external networks, dedicated lines must be used or the data must be encrypted and an authorized person must be at the receiving end prior to the transmission.

Acceptable Delivery of SSA Data. You must deliver SSA data only to authorized personnel and by delivery services that provide tracing services such as certified mail, priority mail or Federal Express. All packages must be properly sealed, labeled and reinforced, and enclosed with a list of the contents being sent.

Destruction of SSA Data. All SSA data not returned must be destroyed by the end of the project date as described in the MOA. SSA data can be destroyed by **burning or shredding**. If the data are burned, use EPA-approved public incinerators to burn it and examine ash residue and re-burn if any large pieces are not totally destroyed the first time. If the data are shredded, use shredders that reduce residue particle size to 3/16 of an inch or less in width.

GUIDANCE FOR PREPARING AN SSA DATA PROTECTION PLAN continued

Explanatory Notes

Clearing Magnetic Media. Magnetic media (tapes, disks, hard drives) containing SSA data must be destroyed or erased prior to reuse. To erase, overwrite SSA data a minimum of three times with a commercial disk utility program. If you are unable to overwrite, degauss using a commercial degausser.

Proper Labeling. All stored or transferred SSA data, electronic or non-electronic, must be labeled **"DISCLOSURE PROHIBITED—THIS CONTAINS SENSITIVE INFORMATION —SSA RESTRICTED DATA."**

Where to Send. Send your completed SSA Data Protection Plan to:

Office of Research, Evaluation,
  and Statistics (ORES)
Social Security Administration
Attn: Division of Earnings Statistics and Analysis
4-C-15 Operations/ c/o 4th Floor Meadows East Building
6401 Security Boulevard
Baltimore, Maryland 21235

AND

For Requesting SSA Program Data for Research
Email the completed SSA Data Protection Plan electronically to
Ores.research.requests@ssa.gov

For Requesting Vital Status (Epidemiological) Data
Email the completed SSA Data Protection Plan electronically to
Ores.epidemiological.requests@ssa.gov