

STANDARD PROCESS A006

Section A: Contract Planning and Administration
Number/Title: A006/Collection and Protection of Personal Information
Date Issued: April 2008
Revision: July 2009
SP Contact: Director, Quality Assurance, non-cGMP, 301-228-4003

I. Purpose

This Standard Process (SP) is to define the requirements and methods used for the collection and protection of personal information.

II. References

THE PRIVACY ACT of 1974 5 U.S.C. § 552a as amended
HHS Chapter 45-13 in the General Administrative Manual
NIH Policy on the Protection of Personally Identifiable Information (PII)
NIH Privacy Awareness Course found in the HHS Learning Management System at:
<https://lms.learning.hhs.gov/>
Federal Information Security Management Act
OMB Circular-A130
SAIC Administrative Policy SG-8

III. Definitions

Personal Information: Any information about an individual, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and information that can be used to trace the identity of the individual, such as a name, Social Security number, address, home phone number, or other identifying number, symbol, or photograph.

Record: Terminology used in the Privacy Act to reference personal information.

SP: Standard Process

System Manager: The individual with overall responsibility for the maintenance and use of a System of Records.

System of Records: A grouping of any records under the control of SAIC-Frederick, Inc., from which information is retrieved by the name of the individual or by some identifying number or identifying particular assigned to the individual, such as a finger or voice print, or a photograph. This does not include a collection of records maintained as a result of management discretion, e.g., personnel records or training files.

System of Records Notice: A document that describes a System of Records. The notice is published in the Federal Register and informs the public as to the types of records maintained and how the records are used, accessed, disclosed, and safeguarded.

IV. Scope

This SP applies to all SAIC-Frederick, Inc., activities that require the collection of personal information in support of operations at the National Cancer Institute at Frederick.

V. Processes/Guidelines

A. Responsibilities

1. Each employee who collects, uses or controls access to personal information has the responsibility for compliance with the requirements specified in this procedure.
2. Managers must ensure that all employees collecting, using, or controlling access to personal information receive appropriate training to understand and fulfill their duties and obligations with respect to privacy and confidentiality.
3. For Systems of Records, each designated System Manager has the responsibility for establishing and implementing appropriate safeguards for an assigned System of Records.
4. The System Manager is responsible for identifying personnel who will have access to system records and ensuring that appropriate training has been provided to these individuals.
5. The System Manager has responsibility for updating the System of Records Notice to reflect any changes to the safeguards used to ensure the security and confidentiality of records contained within each assigned system.

B. Collection of Personal Information

1. Whenever possible, personal information should be collected directly from the subject individual.
2. The subject individual will be informed of the authority for collecting the information, the intended use of the information, and the effect of not providing the requested information.
3. Only the minimum information required to accomplish a specified function should be collected.
4. The subject individual shall be informed that he or she has the right to access and correct and/or amend the information collected.

C. Access Restrictions

1. Only those employees who have an immediate need for the records in order to perform their assigned duties are to have access to the records.
2. Hard copy format
 - a. Access to the personal information must be controlled by physically locating the information in an area that is not accessible to unauthorized personnel.
 - b. An authorized person will be stationed at key access locations during normal business hours.

- c. Authorized users of the personal information must present proper identification (i.e., employee ID badge) prior to receiving access to the information.
 - d. When in use, personal information should not be left unattended. All material should be turned faced down in the presence of visitors or employees who are not authorized users.
 - 3. Electronic format
 - a. Access to systems and data must be protected by a password system.
 - b. When in use, the device containing personal information should not be left unattended.
 - c. Remote access to systems containing personal information requires a 2-factor authentication, i.e., username and password.
- D. Storage Requirements
 - 1. Hard copy format.
 - a. Personal information is not to be left unattended and exposed at any time unless the entire work area can be secured from entry by unauthorized persons.
 - b. Personal information in hard copy format is to be stored in lockable metal file cabinets or in a secured room at all times when not in use during normal business hours, and at all times during non-business hours.
 - 2. Electronic format
 - a. Personal information is to be stored on devices located in a secured area.
 - b. The device should incorporate a time-out function that requires re-authentication after 30 minutes of inactivity.
 - c. Personal information should not be stored on portable devices.
- E. Transfer of Records
 - 1. Personal information is to be transferred in such a way that accidental dissemination will not occur. Sealed opaque envelopes can be used to transfer small volumes of hard copy records. Sealed boxes must be used to transfer large volumes of hard copy records.
 - 2. Personal information must not be transmitted by any electronic means unless it is encrypted and the recipient employee's identity has been fully established.
 - 3. Personal information may not be downloaded to a portable device unless encryption is employed.
 - 4. Personal information may not be printed to a remote printer.
- F. Disaster Plan
 - 1. A written plan for protecting and recovering personal information in the event of a natural disaster or other emergency situation should be maintained. The plan should define processes and procedures for back-up capability to ensure continuity of office operations in the event of an emergency.

VI. Attachments

(NONE)

VII. Records

A. Training Records

1. Any SAIC-Frederick, Inc. employee who collects, accesses or uses personal information must complete the NIH Privacy Awareness Course found in the HHS Learning Management System at: <https://lms.learning.hhs.gov/>. Upon completion of the course, the certificate should be printed and placed in the employee's individual training file.
2. Training records are retained for three years after termination of employment, at which time all records are destroyed.

B. System of Records Notices

1. If the collection of records constitutes a System of Records as defined in the Privacy Act, System of Records Notices will be prepared/updated as defined in the SP entitled, "Preparing and Review of System of Records Notices."
2. Notices are maintained as long as the system is active. Notices are stored in the Contracts Management Office.