**Subject: PRIVACY ACT - BASIC REQUIREMENTS AND RELATIONSHIPS**



## 45-10-00 PURPOSE

A. The Privacy Act of 1974 affects the ways in which the Department and its employees collect, maintain, use, and disseminate information concerning individuals. The prime purpose of the Act is to safeguard personal privacy by limiting and controlling the use of information that Federal agencies collect and maintain on individuals and by providing individuals access to, and the right to amend, records that Federal agencies maintain on them. Chapters 45-10 through 45-19 of the General Administration Manual set forth policies, practices, and procedures for administering those provisions of the Act that apply to Department operations.

B. This initial chapter describes the general framework of responsibility and organization for carrying out these policies, practices, and procedures. It also summarizes the basic requirements of the Act and indicates where in the Department Staff Manual System other instructions applicable to the Privacy Act are located. Other chapters of this Part (45-11 through 45-19) describe specific requirements of the Act and provide guidance for meeting them.

## 45-10-10 POLICY

A. Department policy is to protect the privacy of individuals to the fullest extent possible while at the same time permitting disclosure of records necessary to fulfill the Department's administrative and programmatic responsibilities.

B. In deciding whether to disclose records under the Privacy Act without the written permission of the record subject, the Department is guided by the twelve "conditions of disclosure" exceptions set forth in section (b) of the Act. The most

frequently used of these exceptions by the Department are disclosures made:

1. to Department employees who need the records in the performance of their duties.

2. because the FOIA requires the disclosure. When disclosure under the FOIA may be appropriate, a FOIA Officer, in consultation with the system of records manager, will decide whether to release or withhold records. Normally this involves a balancing process. That is, does the public interest in disclosure outweigh the personal privacy considerations? Public interest in this context is limited to the kind of public interest for which Congress enacted the FOIA, i.e., to shed light on an agency's performance of its statutory duties.

3. for a routine use, as defined and described in the Privacy Act.

## 45-10-20 SCOPE AND APPLICABILITY

This chapter applies to any group of records under the control of the Department from which data on a subject individual are retrieved by a personal identifier assigned to the individual. The identifier may be the name of the subject individual, a number, a symbol, or any other specific retriever assigned to such individual. (See Exhibit 45-10-A for the definition of "individual" within the meaning of this Part.)

## 45-10-30 LEGAL AUTHORITY AND ADMINISTRATIVE GUIDELINES

The provisions of this chapter are based primarily on the following legal authorities and administrative guidelines.

A. Public Law 93-579, known as the Privacy Act of 1974, primarily Sections 3 and 7 of the Act. Section 3 of the Act is codified in the United States Code, Title 5, Section 552a, Records Maintained on Individuals (5 USC 552a). Section 7 relates to the disclosure by individuals of their social security account number.

B. Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, amended the Privacy Act by adding new provisions regulating the use of computer matching. Records produced during the conduct of a matching program are subject to a separate set of requirements.

C. OMB Privacy Act Guidelines of 1975 implementing the provisions of the Privacy Act of 1974 (Federal Register July 9, 1975, p. 28948).

D. OMB Final Guidance of 1989 interpreting the Computer Matching and Privacy Protection Act of 1988 (Federal Register June 19, 1989, p. 25818).

E. OMB Circular No. A-130: Management of Federal Information Resources (Appendix I - Federal Agency Responsibilities for Maintaining Records About Individuals).

F. Department Regulations on the Privacy Act published in the Code of Federal Regulations, Title 45, Part 5b (45 CFR 5b).

## 45-10-40 DEFINITIONS

Key definitions applicable to this chapter and the other chapters on the Privacy Act in Part 45 are located in Exhibit 45-10-A: KEY DEFINITIONS APPLICABLE TO THE PRIVACY ACT. Additional definitions and clarifying information are contained in the definitions paragraphs of section 552a of Title 5 U.S. Code: Records Maintained on Individuals, and the OMB Final Guidance of 1989 Interpreting the Computer Matching and Privacy Protection Act of 1988.

## 45-10-50 ORGANIZATION FOR ADMINISTRATION OF THE PRIVACY ACT WITHIN HHS

A. The Secretary has charged the Assistant Secretary for Public Affairs with the general responsibility for Department-wide implementation and administration of the Privacy Act. The head of each Operating Division (OPDIV) and Staff Division (STAFFDIV) has specific responsibility for the operation of the Act within his organization.-The Secretary, however, has retained approval authority for exempting any system of records from certain requirements of the Privacy Act, in accordance with sections (j) and (k) of the Act.

B. In providing policy guidance, technical assistance, and general oversight, the Assistant Secretary for Public Affairs is assisted by the Director of the FOIA/Privacy Act Division and the HHS Privacy Act Officer within that Division. The HHS Privacy Act Officer coordinates (and serves as a resource to) a network of Privacy Act Officers and Coordinators designated by components of the Department.

C. A system manager, who must be a Department employee, is designated for each Privacy Act system of records maintained

by the Department. This responsible Department official (who is identified in each system of records notice) ensures compliance with the Privacy Act in administering the system of records. If a system of records is relatively small and located in one place, the system manager ordinarily controls access to the records. If the system **is** large or located in more than one place, the system manager may designate other responsible Department officials to control access to the records. Nevertheless, the system manager remains responsible and accountable for the system. Also, an HHS component or office may centralize at one point the control and access to its systems of records. The notice published in the Federal Register for each system of records describes the system and how it is administered.

D. The Secretary of HHS has established an HHS Data Integrity Board to coordinate the implementation of major provisions of the Computer Matching and Privacy Protection Act of 1988. Membership of the Board consists of the Heads of the **OPDIVs** and the following **STAFFDIVs,** or their designated senior level officials:

The Assistant Secretary for Management and Budget

The Inspector General

The Assistant Secretary for Public Affairs.

The Assistant Secretary for Management and Budget (ASMB) serves as Chairperson of the Board. In general, the Board meets at the call of the Chairperson to accomplish duties set forth in the Computer Matching and Privacy Protection Act of 1988 (codified at 5 USC **552a(u)(3)),** establish computer matching policy, and issue guidance to components of the Department.

## 45-10-60 BASIC REQUIREMENTS OF THE PRIVACY *ACT*

A. The basic requirements the Privacy Act places on the Department are summarized here to provide the reader with an understanding of the scope and complexity of the Act and its provisions. They are described in more detail in other chapters **of** this Part 45 and in the administrative guidelines cited in **45-10-30 above.** An agency must:

1. Maintain only information that is relevant and necessary to accomplish an agency purpose required by statute or executive order of the President.

2. Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.

3. Inform each individual of the purpose and use of the information, and any adverse effects of not providing the information sought.

4. Permit an individual to gain access to his record (except in the case of an exempt system of records) and request correction of it.

5. Publish a notice in the Federal Register of the existence and character of each system of records upon establishment or revision.

6. Ensure that all records are sufficiently accurate, timely, relevant, and complete to give the individual a reasonable assurance of fairness in agency uses of the records.

7. Maintain no record describing rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained, or unless pertinent to and within the scope of an authorized law enforcement activity.

8. Notify an individual of any record made available under compulsory legal process when the legal process becomes a matter of public record.

9. Establish employee rules of conduct (and penalties) for persons involved in the design and operation of a system of records, or in maintaining any record.

10. Establish appropriate administrative, technical, and physical safeguards for systems of records.

11. Publish in the Federal Register for public comment any new routine use of the information in a system of records.

B. Computer matching is the computerized comparison of information about individuals for the purpose of determining eligibility for federal benefit programs. In general, matching programs involving federal records must be conducted under a matching agreement between the source and recipient

agencies. The matching agreement describes the purpose and procedures of the match and establishes protections for the records and the individuals involved in the match. The HHS Data Integrity **Board** must approve the matching program before the match may be conducted. A matching agreement may remain in effect for up to eighteen months, and may be renewed for not more than twelve additional months if the matching will be conducted without any change, and each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement. The Secretary of the Data Integrity Board, ASMB, can provide additional information **and** records relating to computer matching requirements and the computer matching programs operating within the Department.

## 45-10-70 PENALTIES

A. The Privacy Act imposes criminal penalties directly on individuals if they knowingly and willfully violate certain provisions of the Act. Any Federal employee, for instance, is subject to a misdemeanor charge and a fine of not more than $5000 whenever such employee:

1. Discloses in any manner records in a system of records to any person or agency not entitled to such records.

2. Maintains a system of records without publishing the prescribed public notice of the system in the Federal Register.

3. Requests or obtains any record from any system of records under false pretenses. (This provision also applies to non-Federal employees.)

B. All HHS employees, especially those who work with a system of records, should be made fully and continually aware of these provisions and their corresponding penalties.

## 45-10-80 OTHER DIRECTIVES PERTINENT TO THE PRIVACY ACT

Additional and more specific instructions for carrying out the provisions of the Privacy Act are located in certain other manuals of the HHS staff manual system, such as the Acquisition Manual, the Information Resources Management Manual, and the Personnel Manual. The subject and location of these instructions **are** listed in Exhibit 45-10-B to this chapter. Questions on privacy materials located in HHS staff manuals should be directed to the responsible HHS staff office. Likewise, whenever HHS employees have questions about the Privacy Act they should

consult with their Privacy Act Officer, **Coordinator, or System** Manager. Legal questions may be brought to the attention of the General Counsel.

## KEY DEFINITIONS APPLICABLE TO THE PRIVACY ACT

The following key definitions are applicable to the Privacy Act and its implementation by this Department. Additional definitions and clarifying information are contained in the definitions paragraphs of section 552a of Title 5, U.S. Code: Records Maintained on Individuals, and the OMB final Guidance of 1989 Interpreting the Computer Matching and Privacy Protection Act of 1988.

1. Access : availability of a record to a subject individual.

2. Agency: the Department of Health and Human Services.

3. Disclosure: the availability or release of a record to anyone other than the subject individual.

4. Individual: a living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. It does not include persons such as sole proprietorships, partnerships, or corporations. A business firm which is identified by the name of one or more persons is not an individual within the meaning of this Part.

5. Maintain: maintain, collect, use, or disseminate when used in connection with the term "record" and to have control over or responsibility for a system of records when used in connection with the term "system of records."

6. Matching program: at its simplest, the comparison of records using a computer. The records must themselves exist in automated form in order to perform the match. Manual comparisons of, for example, printouts of two automated data bases are not included within this definition.

7. Notification: communication to an individual whether he is a subject individual.

8. Recipient agency: any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a computer matching program.

9. Record: any item., collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the

identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

10. Responsible Department official: that official who is identified in a notice of a system of records as the system manager for the system, or another individual. identified in the notice to whom requests *may* be made, or the designee of such officials.

11. Routine use: with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

12. Secretary: the Secretary of the Department of Health and Human Services.

13. Source agency: any agency which discloses records contained in a system of records to be be used in a computer matching program, or any State or local government, *or* agency thereof, which discloses records to be used in a computer matching program.

14. System of records: a group of any records under the control of the Department from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

15. Subject individual: that individual to whom a record pertains.

# HHS DIRECTIVES APPLICABLE TO THE PRIVACY ACT

The additional HHS directives identified below contain further information on the applicability of the Privacy Act to HHS operations. The directives are identified first by the HHS manual in which they are located and then by their specific location within that manual.

## Acquisition Manual

Part 324: Protection of Privacy and Freedom of Information

## Forms Management Manual

Chapter 2-30: Forms Control

## General Administration Manual

Chapter 10-19: Reports Management Compliance with the Privacy Act

## Information Resources Management Manual

Chapter 6-00: Exhibit 6-00-A (Authorities)

## Personnel Manual

HHS Personnel Instruction 297-l: Protection of Privacy in Personnel Records Systems

## Records Management Manual

Chapter 4-10: Use of Federal Records Centers

Subject: SAFEGUARDING RECORDS CONTAINED IN SYSTEMS OF RECORDS



## 45-13-00 PURPOSE

A. The Privacy Act of 1974 requires that each Federal agency establish administrative, technical, and physical safeguards to insure the security and confidentiality of records contained in systems of records and to protect the security and integrity of such records against anticipated threats or hazards. This chapter sets forth minimum safeguarding standards for all such records except records maintained in Automated Information Systems (AIS), i.e., records processed by computer.

B. AIS security requirements are described in the Automated Information Systems Security Program Handbook (issued as Part 6 of the HHS Information Resources Management Manual).

## 45-13-10 SCOPE

The provisions of this chapter apply to all components of the Department, including their contractors, carriers, and intermediaries, that maintain one or more non-automated systems of records, as defined in HHS Exhibit 45-10-A, which are subject to the Privacy Act.

## 45-13-20 RESPONSIBILITIES

A. Each OPDIV, STAFFDIV, and Regional Office is responsible for the application of the minimum standards set forth in this chapter to its non-automated systems of records and for the development and application of any additional standards which are essential to the safeguarding of the records in such systems. These responsibilities include ensuring that subordinate officials and employees carry out the provisions of this chapter.'

B. Each designated system manager has the primary responsibility for the implementation of these standards for the system(s) of records of which he is manager.

C. Each employee who controls physical access to records or disclosure of information contained in the records is responsible for the specific application of these standards to the records under his control.

D. Each OPDIV or STAFFDIV Privacy Act Officer or Coordinator is responsible for providing overall policy guidance and for ensuring that the published notices of systems of records are periodically updated to properly reflect the implementation of appropriate safeguards, including records disposal schedules and methods.

## 45-13-30 DEFINITIONS

The definitions applicable to this chapter are contained in Chapter 45-10 (HHS Exhibit 45-10-A: KEY DEFINITIONS APPLICABLE TO THE PRIVACY ACT).

## 45-13-40 WAIVER PROCEDURE

A. OPDIV and STAFFDIV Heads and Regional Directors may request waivers of specific provisions of these standards. A memorandum requesting a waiver should be addressed to the Assistant Secretary for Public Affairs who is charged with the implementation of the Privacy Act in this Department. The memorandum should describe the nature of the requested waiver, setting forth the rationale supporting the request. This procedure should not be interpreted as providing for a waiver of any provisions of the Privacy Act.

B. The Assistant Secretary for Public Affairs will acknowledge receipt of all requests for such waivers. If the requester does not receive a response within fifteen work days from date of receipt, the waiver should be considered approved.

## 45-13-50 MINIMUM SAFEGUARDING STANDARDS

A. Risk Analysis

1. An analysis of risks to the records in a system of records should be made not less than once every three years to determine what safeguards are essential to maintain the confidentiality and integrity of the records. Such analysis should be updated whenever: there is a significant change in the sensitivity of the

records: new major uses are made of the records; the records are moved from one storage location to another: new equipment is used to process or store the records; or other circumstances indicate possible increased risk to the records. Some factors to be considered in making a risk analysis are:

a. Sensitivity of the records.

b. Nature of facilities, equipment, and total environment in which the records are maintained.

c. Grade level, experience, and training of personnel who are permitted access to the records.

d. Uses which are made of the records, especially decisions on rights, benefits, and privileges.

e. Uses which others could make of the records if they were inadvertently or intentionally disclosed.

f. Harm that disclosure might cause the record subject.

g. Cost of implementing additional safeguards.

2. Any decisions on safeguards should be based on a judgement that considers such factors. The manager of each system of records should maintain a copy of the last risk analysis on which such decisions are based.

B. Access Restrictions

1. Only those employees who have an immediate need for the records in the performance of their official duties are to have access to such records. As a minimum, access to records must be controlled by an arrangement of the following or equivalent standards:

a. Physically locating the records in areas which are not accessible to unauthorized persons.

b. Stationing security personnel or authorized persons at key access locations.

c. Requiring presentation of an authorized form of identification.

2. Before an employee who will control access to records can work with the records, the supervisor or local official in charge must ensure that the employee is familiar with the safeguards applicable to the records, the access standards in effect, and the Employee Standards of Conduct contained in Appendix A to the Department Privacy Act Regulation (45 CFR 5b).

3. Before any other employee can have access to records, the employee must be fully informed about the safeguards in effect while he has possession of the records. The provisions of Appendix A also apply here.

4. The local official who controls access to records contained in a system of records shall:

   a. Maintain a written procedure for restricting access to the records and a list of employees who control access to the records.

   b. Ensure that each employee who controls access to these records is familiar with this written procedure.

   c. Periodically discuss the procedure with these employees to reinforce their understanding and enforcement of access control.

C. Storage Requirements

1. Very sensitive records, such as those relating to a criminal investigation, are to be kept in lockable metal filing cabinets or in a secured room at all times when not in use during working hours, and at all times during non-working hours. (Each system manager should determine whether the records in a system of records are sensitive to this degree.)

2. Other sensitive records are to be kept in closed containers (e.g., filing cabinets or desk drawers) at all times when not in use during working hours and at all times during non-working hours.

3. Alternative storage facilities may be used provided they furnish an equivalent or greater degree of physical security.

4. Records are not to be left unattended and exposed at any time unless the entire work area is secured from entry by unauthorized persons.

D. Transfer of Records

1. Records are to be transferred in such a way that no accidental dissemination will occur. Small volumes of records are to be transferred by mail in sealed opaque envelopes, including interoffice mail. Sealed containers are to be used to transfer large volumes of records.

2. An employee must not transmit information from records by telephone or fax machine to any employee until the employee's identity and need to know are fully established. Call-back or any other effective procedure for establishing identity may be used. Moreover, highly sensitive information should never be transmitted by these means (unless secure telecommunications technology is available) since there is a considerable risk of unauthorized disclosure.

E. Disposal-of Records

Records are to be disposed of in accordance with the General Records Schedules published by the National Archives and Records Service, or in accordance with the supplementary schedules published by components of the Department.

F. Emergency Operating Plan

A plan for protecting and recovering records in the event of a natural disaster, civil disturbance, or other emergency situation should be maintained for each system of records. The plan should provide for sufficient data back-up capability to ensure continuity of office operations. Employees who work with the records should be made aware of their duties under the plan.

## 45-13-60 AUDIT

A. Each OPDIV, STAFFDIV, and Regional Office shall audit each of its systems of records at least once every three years for compliance with the standards set forth in this chapter. This audit may be combined as appropriate with the annual review of record keeping practices required by Appendix I to OMB Circular A-130 (Federal Agency Responsibilities for Maintaining Records About Individuals.).

B. Whenever any standard is not being fully met, the system manager must take action during the audit or immediately thereafter to achieve compliance. The system manager shall maintain a copy of the the last audit report as well as a description of corrective actions taken.