

design, development, operation or maintenance of any system of records as defined herein are informed of all requirements necessary to protect the privacy of individuals who are the subject of such records. All employees shall be informed of all implications of the Act in this area including the civil remedies provided under 5 U.S.C. 552a(g)(1) and the fact that the Corporation may be subject to civil remedies for failure to comply with the provisions of the Privacy Act and this regulation.

(b) The Chief Executive Officer shall also ensure that all personnel having access to records receive adequate training in the protection of the security of personal records, and that adequate and proper storage is provided for all such records with sufficient security to assure the privacy of such records.

**§ 2508.9 What officials are responsible for the security, management and control of Corporation record keeping systems?**

(a) The Director of Administration and Management Services shall have overall control and supervision of the security of all systems of records and shall be responsible for monitoring the security standards set forth in this regulation.

(b) A designated official (System Manager) shall be named who shall have management responsibility for each record system maintained by the Corporation and who shall be responsible for providing protection and accountability for such records at all times and for insuring that such records are secured in appropriate containers whenever not in use or in the direct control of authorized personnel.

**§ 2508.10 Who has the responsibility for maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems?**

The Chief Executive Officer has the responsibility of maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems. These security safeguards shall apply to all sys-

tems in which identifiable personal data are processed or maintained, including all reports and outputs from such systems that contain identifiable personal information. Such safeguards must be sufficient to prevent negligent, accidental, or unintentional disclosure, modification or destruction of any personal records or data, and must furthermore minimize, to the extent practicable, the risk that skilled technicians or knowledgeable persons could improperly obtain access to modify or destroy such records or data and shall further insure against such casual entry by unskilled persons without official reasons for access to such records or data.

(a) *Manual systems.* (1) Records contained in a system of records as defined herein may be used, held or stored only where facilities are adequate to prevent unauthorized access by persons within or outside the Corporation.

(2) All records, when not under the personal control of the employees authorized to use the records, must be stored in a locked metal filing cabinet. Some systems of records are not of such confidential nature that their disclosure would constitute a harm to an individual who is the subject of such record. However, records in this category shall also be maintained in locked metal filing cabinets or maintained in a secured room with a locking door.

(3) Access to and use of a system of records shall be permitted only to persons whose duties require such access within the Corporation, for routine uses as defined in § 2508.4 as to any given system, or for such other uses as may be provided herein.

(4) Other than for access within the Corporation to persons needing such records in the performance of their official duties or routine uses as defined in § 2508.4, or such other uses as provided herein, access to records within a system of records shall be permitted only to the individual to whom the record pertains or upon his or her written request to the Director, Administration and Management Services.

(5) Access to areas where a system of records is stored will be limited to those persons whose duties require work in such areas. There shall be an

## § 2508.11

accounting of the removal of any records from such storage areas utilizing a written log, as directed by the Director, Administration and Management Services. The written log shall be maintained at all times.

(6) The Corporation shall ensure that all persons whose duties require access to and use of records contained in a system of records are adequately trained to protect the security and privacy of such records.

(7) The disposal and destruction of records within a system of records shall be in accordance with rules promulgated by the General Services Administration.

(b) *Automated systems.* (1) Identifiable personal information may be processed, stored or maintained by automated data systems only where facilities or conditions are adequate to prevent unauthorized access to such systems in any form. Whenever such data, whether contained in punch cards, magnetic tapes or discs, are not under the personal control of an authorized person, such information must be stored in a locked or secured room, or in such other facility having greater safeguards than those provided for herein.

(2) Access to and use of identifiable personal data associated with automated data systems shall be limited to those persons whose duties require such access. Proper control of personal data in any form associated with automated data systems shall be maintained at all times, including maintenance of accountability records showing disposition of input and output documents.

(3) All persons whose duties require access to processing and maintenance of identifiable personal data and automated systems shall be adequately trained in the security and privacy of personal data.

(4) The disposal and disposition of identifiable personal data and automated systems shall be done by shredding, burning or in the case of tapes or discs, degaussing, in accordance with any regulations now or hereafter proposed by the General Services Administration or other appropriate authority.

## 45 CFR Ch. XXV (10–1–24 Edition)

### § 2508.11 How shall offices maintaining a system of records be accountable for those records to prevent unauthorized disclosure of information?

(a) Each office maintaining a system of records shall account for all records within such system by maintaining a written log in the form prescribed by the Director, Administration and Management Services, containing the following information:

(1) The date, nature, and purpose of each disclosure of a record to any person or to another agency. Disclosures made to employees of the Corporation in the normal course of their duties, or pursuant to the provisions of the Freedom of Information Act, need not be accounted for.

(2) Such accounting shall contain the name and address of the person or agency to whom the disclosure was made.

(3) The accounting shall be maintained in accordance with a system of records approved by the Director, Administration and Management Services, as sufficient for the purpose but in any event sufficient to permit the construction of a listing of all disclosures at appropriate periodic intervals.

(4) The accounting shall reference any justification or basis upon which any release was made including any written documentation required when records are released for statistical or law enforcement purposes under the provisions of subsection (b) of the Privacy Act of 1974 (5 U.S.C. 552a).

(5) For the purpose of this part, the system of accounting for disclosures is not a system of records under the definitions hereof, and need not be maintained within a system of records.

(6) Any subject individual may request access to an accounting of disclosures of a record. The subject individual shall make a request for access to an accounting in accordance with § 2508.13. An individual will be granted access to an accounting of the disclosures of a record in accordance with the procedures of this subpart which govern access to the related record. Access to an accounting of a disclosure of a record made under § 2508.13 may be