

§ 293.106

the press, and freedom to assemble and to petition the government.

(b) Social Security Number.

(1) Agencies may not require individuals to disclose their Social Security Number unless disclosure would be required;

(i) Under Federal statute; or

(ii) Under any statute, Executive order, or regulation that authorizes any Federal, State, or local agency maintaining a system of records that was in existence and operating prior to January 1, 1975, to request the Social Security Number as a necessary means of verifying the identity of an individual.

(2) Individuals asked to voluntarily (circumstances not covered by paragraph (b)(1) of this section) provide their Social Security Number shall suffer no penalty or denial of benefits for refusing to provide it.

§ 293.106 Safeguarding information about individuals.

(a) To ensure the security and confidentiality of personnel records, in whatever form, each agency shall establish administrative, technical, and physical controls to protect information in personnel records from unauthorized access, use, modification, destruction, or disclosure. As a minimum, these controls shall require that all persons whose official duties require access to and use of personnel records be responsible and accountable for safeguarding those records and for ensuring that the records are secured whenever they are not in use or under the direct control of authorized persons. Generally, personnel records should be held, processed, or stored only where facilities and conditions are adequate to prevent unauthorized access.

(b) Personnel records must be stored in metal filing cabinets which are locked when the records are not in use, or in a secured room. Alternative storage facilities may be employed provided they furnish an equivalent or greater degree of security than these methods. Except for access by the data subject, only employees whose official duties require access shall be allowed to handle and use personnel records, in whatever form or media the records

5 CFR Ch. I (1-1-19 Edition)

might appear. To the extent feasible, entry into personnel record storage areas shall be similarly limited. Documentation of the removal of records from storage areas must be kept so that adequate control procedures can be established to assure that removed records are returned on a timely basis.

(c) Disposal and destruction of personnel records shall be in accordance with the General Record Schedule issued by the General Services Administration for the records or, alternatively, with Office or agency records control schedules approved by the National Archives and Records Service of the General Services Administration.

§ 293.107 Special safeguards for automated records.

(a) In addition to following the security requirements of § 293.106 of this part, managers of automated personnel records shall establish administrative, technical, physical, and security safeguards for data about individuals in automated records, including input and output documents, reports, punched cards, magnetic tapes, disks, and on-line computer storage. The safeguards must be in writing to comply with the standards on automated data processing physical security issued by the National Bureau of Standards, U.S. Department of Commerce, and, as a minimum, must be sufficient to:

(1) Prevent careless, accidental, or unintentional disclosure, modification, or destruction of identifiable personal data;

(2) Minimize the risk that skilled technicians or knowledgeable persons could improperly obtain access to, modify, or destroy identifiable personnel data;

(3) Prevent casual entry by unskilled persons who have no official reason for access to such data;

(4) Minimize the risk of an unauthorized disclosure where use is made of identifiable personal data in testing of computer programs;

(5) Control the flow of data into, through, and from agency computer operations;

(6) Adequately protect identifiable data from environmental hazards and unnecessary exposure; and