

(d) The name, title, and telephone number of the official having operational control over the record; and

(e) If the request is denied in whole or in part, or no record is found in the system, a statement of the reasons for the denial, or a statement that no record has been found, and notice of the procedures for appealing the denial or no record finding.

§ 2606.203 Granting access.

(a) The methods for allowing access to records, when such access has been granted by OGE or the other agency concerned are:

(1) Examination in person in a designated office during the hours specified by OGE or the other agency;

(2) Providing photocopies of the records; or

(3) Transfer of records at the option of OGE or the other agency to another more convenient Federal facility.

(b) When a requester has not indicated whether he wants a copy of the record, or wants to examine the record in person, the appropriate system manager may choose the means of granting access. However, the means chosen should not unduly impede the data subject's right of access. A data subject may elect to receive a copy of the records after having examined them.

(c) Generally, OGE or the other agency concerned will not furnish certified copies of records. When copies are to be furnished, they may be provided as determined by OGE or the other agency concerned.

(d) When the data subject seeks to obtain original documentation, the Office and the other agencies concerned reserve the right to limit the request to copies of the original records. Original records should be made available for review only in the presence of the appropriate system manager or his designee.

Note to paragraph (d) of § 2606.203:

Section 2071(a) of title 18 of the United States Code makes it a crime to conceal, remove, mutilate, obliterate, or destroy any record filed in a public office, or to attempt to do so.

(e) *Identification requirements*—(1) *Access granted in person*—(i) *Current or former employees*. Current or former employees requesting access to records pertaining to them in a system of records may, in addition to the other requirements of this section, and at the sole discretion of the official having operational control over the record, have their identity verified by visual observation. If the current or former employee cannot be so identified by the official having operational control over the records, adequate identification

documentation will be required, e.g., an employee identification card, driver's license, passport, or other officially issued document with a picture of the person requesting access.

(ii) *Other than current or former employees*. Individuals other than current or former employees requesting access to records pertaining to them in a system of records must produce adequate identification documentation prior to being granted access. The extent of the identification documentation required will depend on the type of records to be accessed. In most cases, identification verification will be accomplished by the presentation of two forms of identification with a picture of the person requesting access (such as a driver's license and passport). Any additional requirements are specified in the system notices published pursuant to subsection (e)(4) of the Act.

(2) *Access granted by mail*. For records to be accessed by mail, the appropriate system manager shall, to the extent possible, establish identity by a comparison of signatures in situations where the data in the record is not so sensitive that unauthorized access could cause harm or embarrassment to the individual to whom they pertain. No identification documentation will be required for the disclosure to the data subject of information required to be made available to the public by 5 U.S.C. 552, the Freedom of Information Act. When, in the opinion of the system manager, the granting of access through the mail could reasonably be expected to result in harm or embarrassment if disclosed to a person other than the individual to whom the record pertains, a notarized statement of identity or some similar assurance of identity may be required.

(3) *Unavailability of identification documentation*. If an individual is unable to produce adequate identification documentation, the individual will be required to sign a statement asserting identity and acknowledging that knowingly or willfully seeking or obtaining access to records about another person under false pretenses may result in a criminal fine of up to \$5,000 under subsection (i)(3) of the Act. In addition, depending upon the sensitivity of the records sought to be accessed, the appropriate system manager or official having operational control over the records may require such further reasonable assurances as may be considered appropriate, e.g., statements of other individuals who can attest to the identity of the data subject. No verification of identity will be required of data subjects seeking access to

records which are otherwise available to any person under 5 U.S.C. 552.

(4) *Inadequate identification*. If the official having operational control over the records in a system of records determines that an individual seeking access has not provided sufficient identification documentation to permit access, the official shall consult with the appropriate system manager prior to denying the individual access. Whenever the system manager determines, in accordance with the procedures herein, that access will not be granted, the response will also include a statement of the procedures to obtain a review of the decision to deny access in accordance with § 2606.205.

(f) *Access by the parent of a minor, or legal guardian*. A parent of a minor, upon presenting suitable personal identification as otherwise provided under this section, may access on behalf of the minor any record pertaining to the minor in a system of records. A legal guardian, upon presentation of documentation establishing guardianship and suitable personal identification as otherwise provided under this section, may similarly act on behalf of a data subject declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction. Minors are not precluded from exercising on their own behalf rights given to them by the Privacy Act.

(g) *Accompanying individual*. A data subject requesting access to his records in a system of records may be accompanied by another individual of the data subject's choice during the course of the examination of the record. The official having operational control of the record may require the data subject making the request to submit a signed statement authorizing the accompanying individual's access to the record.

(h) *Access to medical records*. When a request for access involves medical or psychological records that the appropriate system manager believes requires special handling, the data subject should be advised that the material will be provided only to a physician designated by the data subject. Upon receipt of the designation and upon verification of the physician's identity as otherwise provided under this section, the records will be made available to the physician, who will disclose those records to the data subject.

(i) *Exclusion*. Nothing in these regulations permits a data subject's access to any information compiled in reasonable anticipation of a civil action