

(g) *Exception 7.* A Federal, State, or local agency (other than DoD) for civil or criminal law enforcement. The head of the agency or a designee must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. In addition, the "blanket routine use" for law enforcement allows the system manager to disclose a record to a law enforcement agency if the agency suspects a criminal violation.

(h) *Exception 8.* An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.

(i) *Exception 9.* Either House of Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions. The request must come from the committee chairman or ranking minority member (see Air Force Instruction 90-401, Air Force Relations With Congress).<sup>9</sup>

(1) Requests from a Congressional member acting on behalf of the record subject are evaluated under the routine use of the applicable system notice. If the material for release is sensitive, get a release statement.

(2) Requests from a Congressional member not on behalf of a committee or the record subject are properly analyzed under the Freedom of Information Act, and not under the Privacy Act.

(j) *Exception 10.* The Comptroller General or an authorized representative of the General Accounting Office (GAO) to conduct official GAO business.

(k) *Exception 11.* A court of competent jurisdiction, with a court order signed by a judge.

(l) *Exception 12.* A consumer reporting agency in accordance with 31 U.S.C. 3711(e). Ensure category element is represented within the system of records notice.

**§ 806b.48 Disclosing the medical records of minors.**

Air Force personnel may disclose the medical records of minors to their parents or legal guardians in conjunction with applicable Federal laws and guide-

lines. The laws of each state define the age of majority.

(a) The Air Force must obey state laws protecting medical records of drug or alcohol abuse treatment, abortion, and birth control. If you manage medical records, learn the local laws and coordinate proposed local policies with the servicing Staff Judge Advocate.

(b) Outside the United States (overseas), the age of majority is 18. Unless parents or guardians have a court order granting access or the minor's written consent, they will not have access to minor's medical records overseas when the minor sought or consented to treatment between the ages of 15 and 17 in a program where regulation or statute provides confidentiality of records and he or she asked for confidentiality.

**§ 806b.49 Disclosure accountings.**

System managers must keep an accurate record of all disclosures made from any system of records except disclosures to DoD personnel for official use or disclosures under the Freedom of Information Act. System managers may use Air Force Form 771<sup>10</sup>, Accounting of Disclosures. Retain disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.

(a) System managers may file the accounting record any way they want as long as they give it to the subject on request, send corrected or disputed information to previous record recipients, explain any disclosures, and provide an audit trail for reviews. Include in each accounting:

- (1) Release date.
- (2) Description of information.
- (3) Reason for release.
- (4) Name and address of recipient.

(5) Some exempt systems let you withhold the accounting record from the subject.

(b) You may withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request.

**§ 806b.50 Computer matching.**

Computer matching programs electronically compare records from two or

<sup>9</sup> <http://www.e-publishing.af.mil/pubfiles/af/90/afi90-401/afi90-401.pdf>.

<sup>10</sup> <http://www.e-publishing.af.mil/formfiles/af/af771/af771.xfd>.

## § 806b.51

more automated systems that may include DoD, another Federal agency, or a state or other local government. A system manager proposing a match that could result in an adverse action against a Federal employee must meet these requirements of the Privacy Act:

- (1) Prepare a written agreement between participants;
- (2) Secure approval of the Defense Data Integrity Board;
- (3) Publish a matching notice in the FEDERAL REGISTER before matching begins;
- (4) Ensure full investigation and due process; and
- (5) Act on the information, as necessary.

(a) The Privacy Act applies to matching programs that use records from: Federal personnel or payroll systems and Federal benefit programs where matching:

- (1) Determines Federal benefit eligibility;
- (2) Checks on compliance with benefit program requirements;
- (3) Recovers improper payments or delinquent debts from current or former beneficiaries.

(b) Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that won't cause any adverse action are exempt from Privacy Act matching requirements.

(c) Any activity that expects to participate in a matching program must contact Air Force Chief Information Officer/P immediately. System managers must prepare a notice for publication in the FEDERAL REGISTER with a Routine Use that allows disclosing the information for use in a matching program. Send the proposed system notice to Air Force Chief Information Officer/P. Allow 180 days for processing requests for a new matching program.

(d) Record subjects must receive prior notice of a match. The best way to do this is to include notice in the Privacy Act Statement on forms used in applying for benefits. Coordinate computer matching statements on forms with Air Force Chief Information Officer/P through the Major Command Privacy Act Officer.

## 32 CFR Ch. VII (7-1-05 Edition)

### § 806b.51 Privacy and the Web.

Do not post personal information on publicly accessible DoD web sites unless clearly authorized by law and implementing regulation and policy. Additionally, do not post personal information on .mil private web sites unless authorized by the local commander, for official purposes, and an appropriate risk assessment is performed. See Air Force Instruction 33-129 *Transmission of Information Via the Internet*.<sup>11</sup>

(a) Ensure public Web sites comply with privacy policies regarding restrictions on persistent and third party cookies, and add appropriate privacy and security notices at major web site entry points and Privacy Act statements or Privacy Advisories when collecting personal information. Notices must clearly explain where the collection or sharing of certain information is voluntary, and notify users how to provide consent.

(b) Include a Privacy Act Statement on the web page if it collects information directly from an individual that we maintain and retrieve by his or her name or personal identifier (*i.e.*, Social Security Number). We may only maintain such information in approved Privacy Act systems of records that are published in the FEDERAL REGISTER. Inform the visitor when the information is maintained and retrieved by name or personal identifier in a system of records; that the Privacy Act gives them certain rights with respect to the government's maintenance and use of information collected about them, and provide a link to the Air Force Privacy Act policy and system notices at <http://www.foia.af.mil>.

(c) Anytime a web site solicits personally-identifying information, even when not maintained in a Privacy Act system of records, it requires a Privacy Advisory. The Privacy Advisory informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the web page where the information is being solicited, or through a well-marked hyperlink "Privacy Advisory—

<sup>11</sup> <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-129/afi33-129.pdf>.