

(h) *The (k)(7) exemption.* Applies to evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

Subpart L—Disclosing Records to Third Parties

§ 806b.41 Disclosure considerations.

The Privacy Act requires the written consent of the subject before releasing personal information to third parties, unless one of the 12 exceptions of the Privacy Act applies (see § 806b.47). Use this checklist before releasing personal information to third parties: Make sure it is authorized under the Privacy Act; consider the consequences; and check the accuracy of the information. You can release personal information to third parties when the subject agrees in writing. Air Force members consent to releasing their home telephone number and address when they sign and check the “Do Consent” block on the AF Form 624, Base/Unit Locator and Postal Service Center Directory⁷(see Air Force Instruction 33-329, *Base and Unit Personnel Locators*⁸).

§ 806b.42 Social rosters.

Before including personal information such as spouses names, home addresses, home phones, and similar information on social rosters or directories that are shared with groups of individuals, ask for signed consent statements. Otherwise, do not include the information. Consent statements must give the individual a choice to consent or not consent, and clearly tell the individual what information is being solicited, the purpose, to whom you plan to disclose the information, and that consent is voluntary. Maintain the signed statements until no longer needed.

⁷ <http://www.e-publishing.af.mil/formfiles/af/af624/af624.xfd>

⁸ <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-329/afi33-329.pdf>.

§ 806b.43 Placing personal information on shared drives.

Personal information should never be placed on shared drives for access by groups of individuals unless each person has an official need to know the information to perform their job. Add appropriate access controls to ensure access by only authorized individuals. Recall rosters are FOUO because they contain personal information and should be shared with small groups at the lowest levels for official purposes to reduce the number of people with access to such personal information. Commanders and supervisors should give consideration to those individuals with unlisted phone numbers, who do not want their number included on the office recall roster. In those instances, disclosure to the Commander or immediate supervisor, or deputy, should normally be sufficient.

§ 806b.44 Personal information that requires protection.

Following are some examples of information that is not releasable without the written consent of the subject. This list is not all-inclusive.

- (a) Marital status (single, divorced, widowed, separated).
- (b) Number, name, and sex of dependents.
- (c) Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment).
- (d) School and year of graduation.
- (e) Home of record.
- (f) Home address and phone.
- (g) Age and date of birth (year).
- (h) Present or future assignments for overseas or for routinely deployable or sensitive units.
- (i) Office and unit address and duty phone for overseas or for routinely deployable or sensitive units.
- (j) Race/ethnic origin.
- (k) Educational level (unless the request for the information relates to the professional qualifications for Federal employment).
- (l) Social Security Number.

§ 806b.45 Releasable information.

Following are examples of information normally releasable to the public

§ 806b.46

without the written consent of the subject. This list is not all-inclusive.

- (a) Name.
- (b) Rank.
- (c) Grade.
- (d) Air Force specialty code.
- (e) Pay (including base pay, special pay, all allowances except Basic Allowance for Quarters and Variable Housing Allowance).
- (f) Gross salary for civilians.
- (g) Past duty assignments, unless sensitive or classified.
- (h) Present and future approved and announced stateside assignments.
- (i) Position title.
- (j) Office, unit address, and duty phone number (Continental United States (CONUS) only).
- (k) Date of rank.
- (l) Entered on active duty date.
- (m) Pay date.
- (n) Source of commission.
- (o) Professional military education.
- (p) Promotion sequence number.
- (q) Military awards and decorations.
- (r) Duty status of active, retired, or reserve.
- (s) Active duty official attendance at technical, scientific, or professional meetings.
- (t) Biographies and photos of key personnel.
- (u) Date of retirement, separation.

§ 806b.46 Disclosing other information.

Use these guidelines to decide whether to release information:

- (a) Would the subject have a reasonable expectation of privacy in the information requested?
- (b) Would disclosing the information benefit the general public? The Air Force considers information as meeting the public interest standard if it reveals anything regarding the operations or activities of the agency, or performance of its statutory duties.
- (c) Balance the public interest against the individual's probable loss of privacy. Do *not* consider the requester's purpose, circumstances, or proposed use.

§ 806b.47 Rules for releasing Privacy Act information without consent of the subject.

The Privacy Act prohibits disclosing personal information to anyone other

32 CFR Ch. VII (7-1-11 Edition)

than the subject of the record without his or her written consent. There are twelve exceptions to the "no disclosure without consent" rule. Those exceptions permit release of personal information without the individual's consent only in the following instances:

(a) *Exception 1.* DoD employees who have a need to know the information in the performance of their official duties.

(b) *Exception 2.* In response to a Freedom of Information Act request for information contained in a system of records about an individual and the Freedom of Information Act requires release of the information.

(c) *Exception 3.* To agencies outside DoD only for a Routine Use published in the FEDERAL REGISTER. The purpose of the disclosure must be compatible with the intended purpose of collecting and maintaining the record. When initially collecting the information from the subject, the Routine Uses block in the Privacy Act Statement must name the agencies and reason.

NOTE TO PARAGRAPH (C): In addition to the Routine Uses established by the Department of the Air Force within each system of records, the DoD has established "Blanket Routine Uses" that apply to all record systems maintained by the Department of the Air Force. These "Blanket Routine Uses" have been published only once at the beginning of the Department of the Air Force's FEDERAL REGISTER compilation of record systems notices in the interest of simplicity, economy and to avoid redundancy. Unless a system notice specifically excludes a system of records from a "Blanket Routine Use," all "Blanket Routine Uses" apply to that system (see appendix C to this part).

(d) *Exception 4.* The Bureau of the Census to plan or carry out a census or survey under Title 13, U.S.C. Section 8.

(e) *Exception 5.* A recipient for statistical research or reporting. The recipient must give advanced written assurance that the information is for statistical purposes only. NOTE: No one may use any part of the record to decide on individuals' rights, benefits, or entitlements. You must release records in a format that makes it impossible to identify the real subjects.

(f) *Exception 6.* The National Archives and Records Administration to evaluate records for permanent retention. Records stored in Federal Records Centers remain under Air Force control.

(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).⁹

(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 771¹⁰, 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

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

¹⁰ <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 (7-1-11 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*.¹¹

(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—

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

Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used.”

Subpart M—Training

§ 806b.52 Who needs training.

The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. Commanders will ensure that above personnel are trained annually in the principles and requirements of the Privacy Act.

§ 806b.53 Training tools.

Helpful resources include:

(a) The Air Force Freedom of Information Act Web page which includes a Privacy Overview, Privacy Act training slides, the Air Force systems of records notices, and links to the Defense Privacy Board Advisory Opinions, the DoD and Department of Justice Privacy web pages. Go to <http://www.foia.af.mil>. Click on “Resources.”

(b) “The Privacy Act of 1974,” a 32-minute film developed by the Defense Privacy Office. Contact the Joint Visual Information Activity at DSN 795-6543/7283 or commercial (717) 895-6543/7283, and ask for #504432 “The Privacy Act of 1974.”

(c) A Manager’s Overview, What You Need to Know About the Privacy Act. This overview gives you Privacy Act 101 and is available on-line at <http://www.foia.af.mil>.

(d) Training slides for use by the Major Command and base Privacy Act officers, available from the Freedom of Information Act web page at <http://www.foia.af.mil>, under “Resources.”

NOTE: Formal school training groups that develop or modify blocks of instruction must send the material to Air Force Chief Information Officer/P for coordination.

§ 806b.54 Information collections, records, and forms or information management tools (IMT).

(a) Information Collections. No information collections are required by this publication.

(b) Records. Retain and dispose of Privacy Act records according to Air Force Manual 37-139, Records Disposition Schedule.¹²

(c) Forms or Information Management Tools (Adopted and Prescribed).

(1) Adopted Forms or Information Management Tools. Air Force Form 624, Base/Unit Locator and PSC Directory, and AF Form 847, Recommendation for Change of Publication.

(2) Prescribed Forms or Information Management Tools. AF Form 3227, Privacy Act Cover Sheet, Air Force Form 771, Accounting of Disclosures, and Air Force Visual Aid 33-276.

APPENDIX A TO PART 806b—DEFINITIONS

Access: Allowing individuals to review or receive copies of their records.

Amendment: The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer matching: A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential source: A person or organization giving information under an express or implied promise of confidentiality made before September 27, 1975.

Confidentiality: An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identity of confidential sources.

Cookie: Data created by a Web server that is stored on a user’s computer either temporarily for that session only or permanently on the hard disk (persistent cookie). It provides a way for the Web site to identify users and keep track of their preferences. It is commonly used to “maintain the state” of the session. A third-party cookie either originates on or is sent to a Web site different from the one you are currently viewing.

¹² <http://www.e-publishing.af.mil/pubfiles/af/37/afman37-139/afman37-139.pdf>.