Privacy Act (PA) & Personal Identifiable Information (PII)

Proficiency Code: A

What is privacy? Although there is not an official government definition of privacy, it generally refers to the notion of individuals maintaining control over information about them. For the Air Force, the framework of privacy requirements includes the Privacy Act of 1974, the E-Government Act of 2002 (specifically section 208), Office of Management and Budget (OMB) policy, DoD policy, and Air Force policy. Failure to protect privacy can bring about risks to the individual, such as identity theft and risks to the Air Force, such as lawsuits for inappropriate disclosure that divert critical resources away from our mission.

Under the Privacy Act of 1974, 5 U.S.C. § 552a, The Congress finds the following:

The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies. The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information. The opportunities for an individual to secure employment, insurance, and credit, and his/her right to due process, and other legal protections are endangered by the misuse of certain information systems;

The right to privacy is a personal and fundamental right protected by the Constitution of the United States. In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies. The purpose of the Privacy Act is to provide certain safeguards for an individual against an invasion of personal privacy

What information must be protected? The information protected by the various components of the privacy framework is discussed using multiple terms. For the purposes of this Instruction, there are two key definitions to understand:

Personal Information (Personally Identifiable Information (PII))

Office of Management and Budget Memorandum 07-16, Safeguarding Against and Responding to PII Breach - Personally Identifiable Information is defined as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Office of Management and Budget Memorandum10-22, Online Use of Web Measurement and Customization Technologies - The definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to

recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.

For safeguarding of Personal Information, please refer to DoD 5400.11-R, Department of Defense Privacy Program (C1.4, C4 and Appendix 1).

Privacy Act Information is PII which is referred to as personal information that is maintained in a System of Records (SOR) as defined by the Privacy Act, which means the information is retrievable by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Understanding Which Definition Applies. PII is a very broad definition and generally refers to any type of personal information that is linked or linkable to a person. PII may or may not be maintained in a SOR, which means it may or may not also be Privacy Act Information. When PII is maintained in a SOR, it is also Privacy Act Information. Both the Privacy Act requirements and other privacy requirements that protect PII in the privacy framework apply to Privacy Act Information. When PII is not maintained in a SOR, and therefore is not Privacy Act Information, the E-Government Act and many OMB, DoD, and AF policies that protect PII still apply to the information.

To safeguard PII material, digitally sign and encrypt e-mail messages, or password protect any attachments containing personal information.

Paper or electronic documents and/or materials that contain personal information such as a recall rosters, personnel rosters, lists or spreadsheets shall be marked “FOR OFFICIAL USE ONLY” (see DoDM 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI)) as follows:

> *“The information herein is FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 U.S.C 552) and/or the Privacy Act of 1974 (5 U.S.C. 552a). Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties.”*

All paper documents and printed materials that contain personal information shall be covered with the AF Form 3227, Privacy Act Cover Sheet or DD Form 2923, Privacy Act Data Cover Sheet when removed from its approved storage area.

Exercise caution before transmitting personal information via e-mail to ensure the message is adequately safeguarded. Some information may be so sensitive and personal that e-mail may not be the appropriate means of transmitting. (see DoDI 8500.01, Cybersecurity, ECCT-1 (Encryption for Confidentiality (Data at Transmit)).

When transmitting personal information over e-mail, encrypt and add “For Official Use Only” (“FOUO”) to the beginning of the subject line and apply the following statement at the beginning of the e-mail:

> *"This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 U.S.C 552) and/or the Privacy Act of 1974 (5 U.S.C. 552a). Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties. Further distribution is prohibited without the approval of the author of this message unless the recipient has a need-to-know in the performance of official duties. If you have received this message in error, please notify the sender and delete all copies of this message.”*

Do not indiscriminately apply this statement to all e-mails. Use it only in situations when you are actually transmitting personal information required to be protected For Official Use Only purposes. (see DoDM 5200.01, Volume 4 DoD Information Security Program: Controlled Unclassified Information (CUI)) . The guidance in this paragraph does not apply to appropriate releases of personal information to members of the public via e-mail, such as pursuant to the Freedom of Information Act, or with the consent of the subject of the personal information.)

Consult a Records Professional before disposing of any records. You may use the following methods to dispose of records protected by the Privacy Act for authorized destruction according to RDS maintained in the AF Records Information Management System (AFRIMS).

Destroy by any reasonable method that prevents loss, theft or compromise during and after destruction such as pulping, macerating, tearing, burning, shredding or otherwise completely destroying the media so that PII is both not readable and is beyond reconstruction. Refer to NIST SP800-88, http://csrc.nist.gov/publications/PubsSPs.html

Degauss or overwrite magnetic media according to established guidelines. DoDM5200.01, Volume 4, Department of Defense Information Security Program: Controlledictect Unclassified Information (CUI), and AFI 31-401, Information Security Program Management also governs destruction of FOUO and CUI.

Recycling of material protected under the Privacy Act: When safeguarding information protected under the Privacy Act that can be assured; disposal of such products may be accomplished through the Defense Reutilization and Marketing Office (DRMO) or through contracted recycling providers that manage a base-wide recycling program. Originators of material containing PII must safeguard it until it is transferred to the recycling provider. This transfer does not require a disclosure accounting. (Note: Information protected under the Privacy Act shall not be placed in unattended recycle or trash bins.)

Additional Information:
AFI 33-332
AFI 41-200
https://www.privacy.af.mil/

HIPAA and Privacy Act Training (JKO Course DHA-US001).
https://jkodirect.jten.mil/Atlas2/page/desktop/DesktopHome.jsf
This 1-hour course on JKO (Joint Knowledge Online) provides an overview of two critical privacy laws - the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Privacy Act of 1974 - and discusses how these laws are applicable to the Military Health System (MHS). This training provides high-level regulatory standards that apply the same to operations staff, clinical staff, and senior management. It is divided into five modules followed by end-of-module exams. Module 1 provides a general overview of HIPAA, then explores the HIPAA Privacy Rule and correlating DoD Privacy Standards in greater detail. Module 2 focuses on the HIPAA Security Rule as well as DoD's implementation standards. Module 3 provides information about HIPAA Enforcement and HIPAA complaints. Module 4 focuses on the Privacy Act and the DoD Privacy Act Program. And, the final module, Module 5, covers Breach Response at DoD.

Time Burden 1.5 Hours