Frequently Asked Questions - General Information

01. What is the Privacy Act?

The Privacy Act of 1974 establishes a framework of fair information practices that govern how government agencies, including WHS, manage personal records. This legislation stipulates that agencies must collect only information that is pertinent and essential for their functions, refrain from maintaining secret records, and clearly communicate the purpose and intended use of the information at the time of collection. Furthermore, it mandates that records be utilized solely for the stated purposes unless consent is obtained for alternative uses. Agencies are also required to implement sufficient safeguards to protect records from unauthorized access and disclosure, as well as to grant individuals the right to access their records and correct any inaccuracies.

02. Does the Privacy Act apply to all Government records?

No. The Privacy Act is applicable solely to government records that include personal information about individuals, are held by a government agency or its contractors within a system of records, and can be accessed using a personal identifier, such as an individual's name, Social Security Number, medical record number, or another unique identifier.

03. Does the Privacy Act apply to all records maintained about individuals?

No. The Privacy Act is applicable solely to U.S. citizens and lawful permanent residents, and it pertains only to government records that fulfill the specified criteria previously mentioned. It is important to note that the Privacy Act does not extend its protections to individuals who are deceased.

04. What is a System of Records?

A system of records (SOR) refers to a collection of records managed by a Federal government agency, from which personal information about an individual can be accessed using the individual's name or another unique identifier, such as a number or symbol.

05. What is a System of Records Notice (SORN)?

A System of Records Notice (SORN) provides a detailed overview of any records system governed by the Privacy Act. It typically outlines the essential elements such as the identity of individuals involved, the nature of the records, the location of the data, and the purpose behind its collection. Additionally, SORNs explain the procedures available for individuals to access or challenge the information stored about them. Before any data collection—whether in paper or electronic form—can commence, SORNs must be published in the Federal Register to allow for a public comment.

06. Does WHS have any Privacy Act Systems of Records?

Yes. The WHS Privacy Act systems of records may be found at the following site: https://pclt.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/.

07. How does the Government inform the public about the record systems that are covered by the Privacy Act?

The Government notifies the public about record systems governed by the Privacy Act through announcements in the Federal Register. These record systems, known as Privacy Act systems of records, are detailed in the notices, which describe specific systems of records.

08. What are an individual's basic rights and the agency employees' responsibilities under the Privacy Act?

The following is a summary of an individual's rights and the WHS employee responsibilities under the Privacy Act regarding:

A. Collection of Personal Information
Individual Rights: As an individual, when you are asked to provide personal information to a federal agency, you have the right to be informed about several key aspects: the legal basis for the request, the purpose behind the data collection, potential uses of the information, whether your response is mandatory or voluntary, and the implications of refusing to provide the information. As for employees, it is essential to collect only the personal information that is pertinent and necessary for fulfilling an authorized agency function. When requesting such information, you are required to provide written notice to the individual detailing the legal authority for the request, the purpose of the collection, any related uses of the information, and the nature of the response required. This information can be included on a form presented to the individual. Additionally, when asking for a Social Security Number, you must clarify the purpose of the request and whether providing it is mandatory or voluntary. It is advisable to obtain personal information directly from the individual rather than from alternative sources. Furthermore, when collecting a Social Security Number, the agency must complete an SSN Justification Memorandum in accordance with DoDI 1000.30.

B. Access to Records
Individual Rights: Individuals have the right to request access to their records either in writing or in person. It is important to specify the information desired, as general requests for "all information" cannot be accommodated. When visiting in person, proper identification is necessary to confirm the identity of the requester; if suitable identification is unavailable, a written certification of identity will be required. Telephone requests are typically not accepted due to challenges in verifying the caller's identity. Individuals may bring someone with them when reviewing their records, and they are entitled to receive a copy of their record or an acknowledgment of their request within ten working days. While providing a reason for the request is not mandatory, specificity can expedite the response.
As an employee, it is your responsibility to verify the identity of anyone requesting to see their records or to obtain written certification confirming that they are the subject of the request. If a patient wishes to have another person present during the inspection or discussion of their records, prior written authorization from the patient is necessary. Upon receiving a record request, you should determine if a record exists for the individual in a system governed by the Privacy Act. Depending on your organization's procedures, the system manager or their designee must either provide the record or acknowledge the request within ten working days. It is essential not to ask the requester to justify their need to access their own records.

C. Access to Health and Medical Records
Individual Rights: Specific regulations govern access to health and medical records. Generally, individuals have the right to view their medical records directly. However, if there is a possibility that the record contains information that could negatively impact the individual, it will be forwarded to a designated representative, such as a family doctor or another trusted person, who can review the information and relay its contents to the individual. An employee of WHS may also be appointed as this representative.
Employee Responsibilities: When an individual seeks access to their medical record, employees must ensure that the individual designates a representative, such as a family doctor or another qualified professional, who is willing to review the record and discuss its details. A responsible official may assess the medical record and determine that it does not pose an "adverse effect," thereby permitting direct access. It is essential to verify the identity of the individual requesting access, in accordance with the Privacy Act.
be verified.

D. Amendment of Records
Individual Rights: Individuals seeking to amend, delete, or add information to their records must clearly identify the specific record in question and provide justifications for the requested changes. Amendments under the Privacy Act are generally limited to factual and verifiable information; for disputes involving subjective opinions, alternative procedures, such as personnel grievance processes, should be utilized. It is also essential to confirm one's identity as outlined in the relevant guidelines.
Employees are responsible for acknowledging requests to amend records within ten working days, either personally or through an appointed representative, and must inform the requester of the anticipated timeline for a decision. Typically, a review should be completed within 30 days, during which the identity of the requester must be verified. Additionally, any appeals regarding the decision must be resolved within 30 days, with the possibility of a 30-day extension if necessary.
30 days.

09. What can I do to meet my Privacy Act responsibilities?

To ensure the Privacy Act fulfills its goals, it is essential for every employee and contractor handling records with personally identifiable information to collaborate effectively. As a custodian of the information you manage, it is your responsibility to understand the Privacy Act's requirements as they pertain to your role. This understanding can be gained through formal training, on-the-job experiences, discussions with your supervisor, and thorough reading of relevant policies and procedures. Additionally, you should evaluate your methods of handling personal information and implement necessary safeguards to protect it. Certain staff members within WHS are specifically trained in the Privacy Act, and your supervisor can direct you to the appropriate Privacy Act official for assistance. It is also crucial to respond swiftly to information requests by referring them to the designated WHS Privacy Act official and to familiarize yourself with the procedures for such requests. Lastly, be vigilant in ensuring that personal information is not disclosed without prior consent from the individual concerned or unless legally authorized, as the Privacy Act permits access to records only for WHS employees with a legitimate need in the course of their duties.

10. Does the Privacy Act apply to all WHS employees?

Yes. As a WHS employee, you have dual roles to navigate. On one side, you are a private citizen entitled to the protections and rights under the Privacy Act. On the other, you are a federal employee responsible for handling records that contain personal information, which includes adhering to legal obligations. Unless you hold the position of a Privacy Act system manager or a designated representative, you must refrain from disclosing any information protected by the Privacy Act or granting unauthorized individuals access to such records. The gravity of this duty is underscored by the significant penalties associated with violations, which can include fines of up to $5,000 for willful disclosures of personal information. Additionally, disciplinary measures for breaches may range from reprimands to suspension or even termination of employment.

11. Does the Privacy Act apply to contractors?

Yes, when a contractor creates or maintains a system of records for the purpose of managing WHS records, it is essential to include specific clauses in the solicitations and contracts. These clauses ensure that the necessary legal and operational standards are upheld throughout the duration of the contracts: 52.224-1, Privacy Act Notification and 52.224-2, Privacy Act.

12. What does it mean to make a routine use disclosure from a Privacy Act System of Records?

A routine use disclosure under the Privacy Act allows for the sharing of information from a record with external requestors without needing the consent of the individual to whom the record relates. Such disclosures must align with the original purpose for which the information was collected and are required to be published in the Federal Register.

13. What is "Personally Identifiable Information (PII)"?

Personal Identifiable Information (PII) encompasses data that can be used to identify or trace an individual. This includes details such as a person's name, social security number, date and place of birth, mother's maiden name, biometric data, home phone numbers, and various demographic, personnel, medical, and financial records. PII refers to any information that is either directly linked to an individual or can be associated with them when combined with other personal or identifying details.

14. What is Identity Theft?

Identity theft is an increasingly prevalent crime that takes advantage of personal information to create fraudulent accounts or gain unauthorized access to existing ones. This can result in significant financial burdens, as identity thieves may rack up substantial debts in your name, leaving you and your family responsible for the consequences. Furthermore, the repercussions extend to your credit history, potentially hindering your ability to secure loans or even employment in the future. In some cases, criminals may engage in illegal activities under your identity, which could lead to a tarnished criminal record. Often, identity theft originates from seemingly innocuous situations, such as a lost wallet or checkbook, or compromised personnel records that provide thieves with a wealth of personal data. The sources of identity theft are diverse and can arise from various circumstances, such as:

The theft of mail, checks, or personal records. One common tactic is dumpster diving, where criminals sift through discarded items to find bills or sensitive documents. Additionally, by manipulating change of address requests, thieves can reroute important mail such as bank statements and credit offers, gaining access to personal information and accounts. Phishing is another prevalent technique, involving deceptive emails that appear to be from legitimate financial institutions, prompting individuals to provide personal details. This can also involve directing victims to counterfeit websites designed to mimic trusted organizations. Furthermore, skimming poses a risk at familiar retail locations, where advanced card readers can capture credit card information during routine transactions, often facilitated by staff who may save this data for future exploitation.

15. What should I do if I suspect my identity has been stolen?

Addressing the repercussions of identity theft can be a complex endeavor, and acting swiftly is crucial. For detailed guidance on the necessary actions to take following an incident of identity theft, it is advisable to consult the Federal Trade Commission's website at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

16. What are Privacy Impact Assessments (PIAs) and where can I find them?

A Privacy Impact Assessment (PIA) is essential for Department of Defense (DoD) Information Technology (IT) systems and electronic collections that handle Personally Identifiable Information (PII). This assessment ensures that the management of PII aligns with relevant legal, regulatory, and policy standards concerning privacy. It also evaluates the necessity, privacy risks, and implications associated with the collection, maintenance, usage, and dissemination of PII in electronic formats. Furthermore, the PIA scrutinizes existing protections and explores alternative methods to reduce potential privacy risks. This process is applicable when PII related to the public, including DoD personnel, contractors, or foreign nationals at U.S. military installations abroad, is collected, maintained, used, or shared electronically. It also extends to DoD IT systems and electronic collections that involve external contracts for the handling of such information.

The WHS Privacy Impact Assessments (PIAs) can be accessed on the WHS Privacy Website, and on the DoD CIO SharePoint Site at https://dodcio.defense.gov/PIA/. For further guidance on PIAs, including DODI 5400.16 and the DD Form 2930, please visit the same DoD CIO SharePoint Site.