

PRIVACY ACT INFORMATION

What is considered privacy information requiring protection under the Privacy Act Law of 1974? The definition used by the Department of the Navy (DON) for Protected Personal Information (PPI) is “any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history; information which can be used to distinguish or trace an individuals identity such as their name, social security number (SSN), date and place of birth, mothers maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.” Additional PPI data includes:

- Security clearance level.
- Leave balances; type of leave used.
- Home address and telephone numbers (including home web addresses).
- Drug test results and the fact of participation in rehabilitation programs.
- Family data.
- Religion, race, national origin.
- Performance ratings.
- Names of employees holding government-issued travel cards, including card data.

As can be seen, PPI covers a very large spectrum of information. This includes some things we might not think about as being covered by the Privacy Act Law. This includes reports from the Automated Training Management System (ATMS) and many of the forms we use here at the Shipyard and IMF. Some of the forms we use on a daily basis contain privacy information (i.e. SSN number). The frequency that some of these forms are used may lead us to be less vigilant in guarding the information they contain. Some of these forms are:

- Special Achievement Award Recommendation
- Claim for Reimbursement for Expenditures on Official Business
- DON Student Loan Repayment Application
- Electronic Funds Transfer
- Employee Address Change
- Employee/Emergency Contact Record
- Performance Appraisal Review Process (PARPs), Supervisory and Non-Supervisory
- Transportation Incentive Program (TIP) Forms
- Standard Sailing List Data (Sea Trial Rider List)
- Student Loan Repayment Service Agreement
- Leave Recipient Application Under Voluntary Leave Transfer Program
- Request to Donate Leave Under Voluntary Leave Transfer Program
- Direct Deposit Sign Up Form
- Temporary Duty Time and Attendance Report
- Leave and Earning Statements

This list is ***NOT*** all-inclusive. These are just some of the forms used every day here at the Shipyard and IMF. As can be seen, these forms cover a wide range of usage and many of them could very easily be accidentally left where some one, not authorized for that specific information about an individual, could have access to the information. This is what we, as DON employees, must guard against.

As DON employees we have an obligation and a requirement to ensure DON complies with all provisions of the Privacy Act. Here are things you should be doing (or not doing) to prevent disclosure of Privacy Act information:

- DO NOT collect personal data without authorization.
- DO NOT maintain illegal files; do not maintain inaccurate information.
- DO NOT distribute or release personal to other employees unless you are convinced they have an official need-to-know. An example of this would be to answer questions about an individual as part of a security investigation to determine if that person can have a security clearance.
- DO NOT be afraid to challenge “anyone” who asks to see Privacy Act information for which you are responsible.
- DO NOT maintain records longer than permitted.
- DO NOT place unauthorized documents in Privacy Act system records.
- DO NOT commingle information about different individuals in the same file.
- DO NOT transmit personal data without ensuring it is properly marked. Use ‘FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE.’
- Ensure that you mark all documents that contain privacy information as “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE”
- DO NOT place privacy data on shared drives, multi-access calendars, the Intranet or Internet.
- If you get a written or verbal request for information or records, forward it to the Shipyard Legal Office, Code 107.

Privacy Act information should be marked (paper records and e-mails): “For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties.” We must be aware that Privacy Act data may not always be marked as such. If you have any questions about whether data is protected under the Privacy Act, always ask your supervisor.

Unauthorized disclosure of Privacy Act information carries criminal and civil penalties.

Criminal Penalties - If you commit one of the following violations you can be charged with a misdemeanor and fined not more than \$500.00:

- Willfully disclose individually identifiable information to any person or agency not entitled to receive it.
- Maintain records that can be retrieved by an individual’s name, social security number, payroll number, or any other personal identifier unless a notice has been published in the Federal Register.
- Knowingly and willfully obtain any record concerning an individual from an agency under false pretenses.

Civil penalties – An individual may bring a civil action against an agency in the district courts of the United States for violations of the Privacy Act. If the court determines that the agency acted in a manner that was intentional or willful, the United States can be liable in an amount equal to the sum of actual damages sustained by the individual, not less than \$1000.00, and the cost of the suit together with reasonable attorney fees. Violations that can incur civil penalties are:

- Unlawfully refuse to amend a record.
- Unlawfully refuse to grant access to records.
- Fail to maintain accurate, relevant, timely and complete data.
- Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect.

General rules for handling Privacy Act Information:

- DON'T leave privacy data in the open for anyone to view.
- Ensure privacy data is not accessible to individuals that do not have an official need to know.
- DON'T store privacy data in a public folder.
- Dispose of privacy data by any method that renders the information unrecognizable or beyond reconstruction. This includes but is not limited to:
 - Tearing
 - Burning
 - Pulping
 - Shredding
 - Burning
- Before disseminating Privacy Act data, make sure it is marked to alert the receiver as to the sensitivity of the information.
- DON'T use yard mailers (holey joes) or messenger-type envelopes to mail privacy data. Double wrap using an inner and outer envelope if you think it is appropriate. Never indicate on the outer envelope that it contains privacy data.
- Use Common Access Card procedures and announce in the opening line of text that you are relaying FOUO information when e-mailing privacy data.
- Place paper records containing Privacy Act data shall be placed in locked drawers, locked briefcases, or other secure areas where family or household members cannot see it. Use password protection protocols for electronic records.
- DON'T dispose in regular trash.
- Immediately notify your supervisor, Privacy Act Officer (Code 107), or any other appropriate official of accidental inappropriate disclosures of Privacy Act data. If it was released to the World Wide Web, make a note of where the information was posted by copying the URL listed at the top of the screen.
- Take privacy protection seriously.
- Respect the privacy of others.
- Alert your supervisor or other management official when you see personal data left attended.
- KNOW the Privacy Act requirements as set forth in PSNS&IMFINST 5211.1F and SECNAVINST 5211.5E