

Definition of PII

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity. Examples include but are not limited to: Name, Social Security number (SSN), date of birth, home address, home phone number, personal e-mail address, financial information, fingerprints, photograph, medical information, and civilian National Security Personnel System (NSPS) data.



Collecting PII

If you collect, maintain or use Personally Identifiable Information, it must be needed to support a DON function or program as authorized by law, Executive Order or operational necessity. Whether you are working from your desk at the office, at home, at sea, or in the field, it is your responsibility to:

- Ensure that the information entrusted to you in the course of your work is kept secure and protected.
- Minimize the use, display or storage of SSNs and other PII whenever possible.
- Keep the information timely, accurate and relevant to the purpose for which it was collected.
- Allow only those personnel with "a need to know" access to PII.
- Immediately notify your supervisor if you suspect or discover that PII has been lost or compromised.

IT Equipment

a Never leave your laptop unattended.

- Keep your laptop in a secure government space or secured under lock and key when not in use.
- Laptops and mobile electronic equipment must have full disk encryption.
- Mark all external drives or mobile media with "FOUO, Privacy Sensitive."
- As a best practice, do not create, store or transmit PII on IT equipment when the information is not encrypted.
- Ensure PII resides only on government furnished IT equipment. Never store PII on personal devices.
- Do not maintain PII on a public Web site or electronic bulletin board.

E-mail

- E-mail containing PII must be digitally signed and encrypted using DoD-approved certificates.
- As a best practice, ensure the e-mail subject line contains "FOUO Privacy Sensitive" if the document contains PII.
- Ensure the body of the e-mail contains the following warning, "For Official Use Only. Privacy Sensitive Information. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- Double-check that you have the correct e-mail addresses before sending.
- **Double-check** your attachment to make **sure** you have selected the right document.
- Phishing is a growing concern; ensure you open **and** respond to legitimate sources only.

Printed Materials & Fax Machines

- ❑ Verify printer location before sending a document containing PII to the printer.
- ❑ Promptly pick up all copies of the documents as soon as they are printed.
- ❑ Double-check the fax number before faxing documents with PII.
- ❑ Ensure someone is standing by on the receiving end of the fax.
- ❑ Ensure all printed documents with PII are properly marked with “FOUO, Privacy Sensitive.”
- ❑ As a best practice, transport/hand carry PII documents in a double wrapped container/envelope. Use a DD Form 2923 “Privacy Act Data Cover Sheet” as a cover.

- ☑ *80% of all DON PII breaches are due to human error.*
- ☑ *80% of all DON PII breaches involve the loss or compromise of SSNs.*
- ☑ *ID theft affected 8 million adults in the U.S. in 2007.*
- ☑ *Social Security numbers are the most valuable commodity for an identity thief.*
- ☑ *Risk is greatest when PII is stolen by a hacker or thief, but the insider threat is growing.*
- ☑ *ID theft crimes occur more often offline than online, but the trend is changing.*

Disposal

- ❑ Dispose of documents containing PII by making them unrecognizable by shredding or burning.
- ❑ As a best practice, before turn-in, ensure all hard drives are properly marked, physically destroyed, and actions documented.
- ❑ Do not discard documents containing PII in trash or recycle bins.
- ❑ Copiers and printers use hard drives and must be properly sanitized.

Network Shared Drives

- ❑ Make sure that controls are in place to limit access to files/folders that contain PII to those with a “need to know.”

- ❑ Limit storage of PII on shared drives and folders whenever possible.
- ❑ Delete files containing PII in accordance with the SECNAV Records Management Manual.
- ❑ Verify that access controls are restored after maintenance.

Compliance

- ❑ All DON personnel who handle PII must complete annual PII training, and the command must maintain auditable certificates of completion.
- ❑ All offices that handle PII must complete a Compliance Spot Check twice yearly, and the command must maintain auditable records.

Reporting Incidents

- ❑ Contact your privacy act coordinator or supervisor as soon as you suspect or have an actual loss or compromise of PII.
- ❑ Report PII breaches within one hour of discovery to US-CERT and your chain of command in accordance with DON CIO or Marine Corps guidance.
- ❑ Upon receipt of a PII Breach Report, DON CIO will provide the reporting command with a written notification determination.
- ❑ If your PII is compromised, monitor financial accounts for suspicious activity.
- ❑ If your identity is stolen, contact the Federal Trade Commission at www.ftc.gov or 1-877-IDTHEFT.