SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)
BEST PRACTICES

DoD 5400.11-R defines Personal Information as: Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as <u>personally identifiable information</u> (i.e. information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked to likable to a specified individual).

<u>Your Responsibilities to Safeguard PII</u>

PII in the office

DO:
- ✓ Prevent unauthorized persons from having access to PII. This includes co-workers.
- ✓ Escort visitors.
- ✓ Use a Privacy cover sheet.
- ✓ Pick up and safeguard documents containing PII if you find it unprotected.
- ✓ Keep PII locked in a desk drawer, file cabinet or office if you are away from your desk.
- ✓ Look for unprotected PII during "end of day checks."

DON'T:
- ✗ Email PII outside the .mil domain.
- ✗ Discuss PII near unauthorized personnel.
- ✗ Release PII to anyone unless specifically authorized to do so in order to perform official duties.
- ✗ Forget to clear office equipment of printed paper or paper jams, especially if it contains PII.
- ✗ Forget to remove your CAC from your computer if you leave your desk.
- ✗ Access PII unless you have a need to know requirement in the performance of your duties.

Sharing PII

DO:
- ✓ Encrypt all emails containing PII.
- ✓ Enforce "Need to Know."
- ✓ Validate the recipient of the PII requires the PII for an official DoD purpose.
- ✓ Use caution when emailing to distribution lists or group emails

DON'T:
- ✗ Share PII using non DoD approved computers or private email accounts e.g. yahoo.com.
- ✗ Share PII with anyone not authorized to have the PII.
- ✗ Forget, the recipient of a document/email may not be authorized to access the PII in the document/email – Remove the PII.
- ✗ Post PII to shared work sites unless access controls can be applied.

Securing PII

DO:
- ✓ Use a Burn Bag to destroy PII.
- ✓ Store PII only in approved DoD work locations.
- ✓ Ensure PII in documents/email is specifically marked with "For Official Use Only – Privacy Act Data."
- ✓ Encrypt email containing PII before hitting SEND.
- ✓ Ensure laptops and mobile devices where PII is stored are encrypted.

DON'T:
- ✗ Discuss PII in non DoD approved work locations e.g. restaurant; car pool; public transportation; your doctor's office; hallways.
- ✗ Store PII in non DoD approved locations, e.g. your car.
- ✗ Leave laptop compters or mobile computing devices in any vehicle
- ✗ Toss documents containing PII in a trash can or recycle bin.

Telework w/PII

DO:
- ✓ Access and process PII only through a DoD approved laptop/computer.
- ✓ Prevent family and friends from having access to your laptop/computer.

DON'T:
- ✗ Email PII to a personal email account e.g. yahoo.
- ✗ Use your personal computer to process PII.
- ✗ Take home paper/CDs containing PII.

PII Reporting

DO:
- ✓ Contact security@whs.mil if you have any questions or to report failures to safeguard PII.
- ✓ Take corrective action if you can to prevent a "breach" from occurring.
- ✓ Report known or suspected instances of any failure to protect PII.

DON'T:
- ✗ Avoid your responsibility to safeguard PII.

For more information on the Department of Defense Privacy Program visit: http://dpclo.defense.gov/privacy/