HANDBOOK FOR SAFEGUARDING PII

HOW TO SAFEGUARD SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

This fact sheet helps you safeguard **Sensitive Personally Identifiable Information (PII)** in paper and electronic form during your everyday work activities. USNA employees, contractors, consultants, interns, and midshipmen are required by law and USNA policy to properly collect, access, use, safeguard, share, and dispose of PII in order to protect the privacy of individuals.

What is PII?

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. (OMB Circular No. A-130) ***Sensitive PII requires stricter handling guidelines, which are detailed by USNA's Privacy Program Instruction 5211.3 series and summarized below.***

Sensitive and Non-Sensitive PII. For purposes of determining whether individual notifications would be required if there were a PII breach or whether a Privacy Impact Assessment (PIA) was required for an IT system that collects PII, PII elements are categorized as sensitive PII (i.e., if this information was lost or compromised it could potentially result in harm or identity theft) or non-sensitive PII, also known as Internal Government Operations or business related PII, (i.e., the risk of harm or identity theft associated with the loss or compromise would be minimal to non-existent). Non-sensitive PII is normally considered releasable to the public per DoD 5400.11-R (see paragraph C4.2.2.5).

The following matrix is intended to assist in determining if information is Sensitive or Non-Sensitive PII for use in internal DoD operations. While this list is not all-inclusive, it is intended as a reference only. If there is any doubt as to the sensitivity of PII, contact the Privacy Officer for clarification or treat it as Sensitive PII.

INFORMATION	SENSITIVE PII	NON-SENSITIVE PII
The following elements are considered PII whether alone or combined with additional PII (No G-drive):		
Social Security Number (SSN) in any form (full, truncated, masked)	X	
Biometric Data (fingerprints, DNA, iris scan)	X	
Personal Identification Number (passport, driver's license, other ID)	X	
Financial Information (credit card numbers, account numbers)	X	
Identity of an individual in conjunction with any of the below:		
Sex, race, ethnicity, or religious affiliation	X	
Date and/or place of birth	X	
Personal phone numbers*, email addresses, and home address	X	
Grades**	X	
Mother's middle name, maiden names, and/or alias	X	
Spouse, marital, child, and emergency contact information	X	
Passwords	X	
Citizenship/Immigration and/or Legal Status	X	
Salary and bonus information	X	

INFORMATION	SENSITIVE PII	NON-SENSITIVE PII
Identity of an individual in conjunction with any of the below:		
Medical data and protected health information (PHI) (diagnosis, treatment, history)	X	
Law Enforcement Information	X	
Military Records (sensitive duty stations, security clearance, fitreps, urinalysis results…)	X	
Employment and Education Information (performance ratings, pay pool, transcripts)	X	
Information Identifying Personal Property (Vehicle registration, title number)	X	
Name***		X
Office name and location***		X
Work/business phone numbers and fax		X
Work/business address (mailing and email)		X
Job title, pay grade, and rank		X
Assigned position/ Billet information		X
DoD ID number, DoD Benefits number, and or lineal number		X
Schedules that do not include Sensitive PII***		X
Major or field of study		X
Participation in Extra Curricular Activities and Sports		X
Alpha code/ candidate number		X
Company or battalion		X
Rosters*/****	X	X

***Personal Phone Numbers**

- Lists of personal phone numbers should always be treated as sensitive PII. Personal phone numbers collected on official forms or officially should be kept in accordance with the governing System of Records Notice (SORN). This can be found on the Privacy Act Statement (PAS) used to collect the information.
- Personal numbers listed in signature blocks or sent unsolicited as business related contacts are treated as work PII and may be sent unencrypted to those with a lawful government purpose to access the information.

****When creating and sharing grades or grading reports, you should:**

- Never share grade information with faculty, staff, or midshipmen who do not have a "need to know."
- Never post grades where people without a "need to know" have access to them (applies to all types of grades - quiz, mid-term, final, homework). This applies to hard copies and electronic postings.
- Never leave graded assignments in a stack for students to pick unless they are sealed in envelopes with the student's name on it and someone remains in the room to ensure all assignments have been claimed. You may also leave them with an assistant (non-midshipmen) or receptionist to hand out.
- Lists of final grades and any official documents containing grades should always be considered Sensitive PII (transcripts).
- When emailing individual midshipmen about academic related information, progress, assignments, status of course grades, etc., you can email them using the Google interface as long as it remains within the usna.edu network. This does not include copies of transcripts and only pertains to class related information with only those with a need to know included on the email (instructor, subject midshipman, academic adviser, company officer...)

*****Names, Locations, Schedules...**

- Real world threats must be considered when disclosing lists of names of DoN personnel (faculty, staff, and midshipmen) outside the DoD environment. Likewise, if an individual's location, schedule, or job assignment poses a privacy or security threat, public disclosure is prohibited.

******When creating and sharing a recall roster, you should:**

- Ask: Does the recipient(s) have a need to know? Is the information appropriately marked as "*CUI*"? Is the transmission secure? Should the information be displayed in this location? Are only essential PII elements listed?
- Ensure that the sole purpose of a roster is to recall personnel and/or notify them of building closings.
- Limit PII elements to only the minimum required to recall an individual, e.g., names, addresses and telephone numbers (home, work, cell phone). SSNs should never be included.
- Provide a Privacy Act Statement any time PII is solicited from an individual, whether in writing or electronically. Contact your Privacy Act coordinator for more information.
- See *CNO Memorandum: "Recall Rosters"* for additional information.

Guidelines for Safeguarding Sensitive PII

I. Collecting and Accessing Sensitive PII

Before collecting or maintaining Sensitive PII, be sure that: (1) you have the authority to do so; (2) the data collection is consistent with the terms of a Privacy Act System of Records Notice (SORN); and (3) your database or information - technology system has an approved Privacy Impact Assessment. Access to Sensitive PII is based upon your having an official need to know, i.e., when the information relates to your official duties. Limit your access to only the Sensitive PII needed to do your job.

- Ensure that casual visitors, passersby, and other individuals without an official need to know cannot access or view documents containing Sensitive PII. If you leave your work area for any reason, lock your computer's screen.
- Ensure privacy while having intra-office or telephone conversations regarding Sensitive PII.
- Do not post Sensitive PII on the USNA Intranet, the Internet, social networking sites, shared drives, SharePoint, or multi-access calendars accessible to individuals without an official need to know or proper authorization.
- Do not share account information, especially logins or passwords, with anyone. Do not have login or password information accessible to others (such as on a sticky note on your computer).
- Be alert to phone calls or emails from individuals claiming to be USNA employees attempting to gather or verify personal or non-public information. USNA will never ask you to verify your account login, password, or personal information by email or over the phone.

II. Using and Safeguarding Sensitive PII

***Limit duplication of Sensitive PII*:** Before creating new spreadsheets or databases that contain Sensitive PII from a larger file or database, consult the *USNA Privacy Office*.

***Protect hard-copy Sensitive PII*:** Do not leave Sensitive PII unattended on desks, printers, fax machines, or copiers. Secure Sensitive PII in a locked desk drawer, file cabinet, or similar locked enclosure when not in use. When using Sensitive PII, keep it in an area where access is controlled and limited to persons with an official need to know. Avoid faxing Sensitive PII if other options are available.

***Safeguard USNA media*:** Sensitive PII may only be saved, stored, or hosted on USNA-approved portable electronic devices (PEDs), such as laptops and tablets. All portable media must be encrypted pursuant to *USNA Privacy Program Instruction 5211.3 series*. If you need to transport your laptop or PED and must leave it in a car, lock it in the trunk and out of sight. Do not leave your laptop or PED in a car overnight. If lost or stolen, immediately report the missing asset to USNA's Privacy Officer. The below diagram, elaborates on where sensitive information can be stored.

Storing PII on the shared drive: Store Sensitive PII on shared access computer network drives ("shared drives") only if access is restricted to those with a "need to know" by permissions settings or passwords. This is the preferred storage location for PII. Contact USNA's Information Technology Services Division to set-up permissions and restrict access to a shared file or folder.

Storing PII on the Google drive: The USNA CIO has authorized the following for the G-Suite and Drive:

1. Storing the following PII in USNA Google G Suite Drive and USNA Google Shared Drive is PROHIBITED in any quantity:

a. Social Security Number
b. Driver's License Number
c. Financial Account Number
d. Passport Number
e. Fingerprint
f. Iris scan

2. Storing the following PII in USNA Google G Suite Drive and USNA Google Shared Drive is PROHIBITED in any quantity when the data is associated with any part of an individual's name:

a. Truncated Social Security Number
b. Date of birth
c. Citizenship or immigration status
d. Ethnic or religious affiliation
e. Sexual orientation
f. Criminal history
g. Medical history, mental condition, medical treatment, medical diagnosis
h. Mother's maiden name
i. Account password or PIN

III. Sharing Sensitive PII

You are authorized to share PII within the agency (DoD) with those with a "need to know" in the performance of their duties. If you are in a position that requires you to share/disclose PII for any other reason authorized in 5 U.S.C 552a(b), a record of disclosure must be kept in accordance with 5 U.S.C 552a(c). Only the Freedom of Information Act (FOIA) Officer will release information pursuant to the FOIA (5 U.S.C 552).

Emailing Sensitive PII

You may email Sensitive PII to a recipient with an official need to know, but your email must be signed and encrypted. In addition to digitally signing and encrypting emails containing PII, the body of the email, including any email attachments containing PII, must be marked properly (i.e., "CUI" per *DoDI 5200.48 series.)*

The Google (G-mail) interface is NOT authorized for emailing Sensitive PII. You can either use the Outlook interface or DoD SAFE to send Sensitive PII via email.

Finally, before emailing Sensitive PII, confirm that you have the correct email address.

***Never email Sensitive PII to personal email accounts*:** Personal computers should not be used to access, save, store, or host Sensitive PII.

Mailing Sensitive PII

Encrypt Sensitive PII stored on CDs, DVDs, hard drives, floppy disks, and other removable media prior to mailing or sharing. Also, ensure that the media is properly labeled.

Always verify that the recipient received the information. Note that FOIA requests may require different handling. Always Seal Sensitive PII in an opaque envelope or container. Use First Class Mail, Priority Mail, or a traceable commercial delivery service (UPS, FedEx).

Double wrap mail consisting of more than 25 individual's Sensitive PII. Affix CUI markings or Privacy Act Cover Sheet to the outside of the inner envelope. Do not put CUI markings on the outer envelope when mailing.

IV. Disposing of Sensitive PII

Sensitive PII, including that found in archived emails, must be disposed of when no longer required, consistent with the applicable records disposition schedules. If destruction is required, take the following steps:

- Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction. Shred paper containing Sensitive PII using a cross cut shredder; do not recycle or place in garbage containers. Be especially alert during office moves and times of transition when large numbers of records are at risk.
- Before transferring your computer or PED to another employee, ask your Help Desk to sanitize Sensitive PII from computer drives and other electronic storage devices.
- Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

V. Reporting Privacy Incidents

You must **immediately** report all suspected or confirmed privacy incidents involving the loss or compromise of all PII to your supervisor and the Privacy Coordinator. If your supervisor is unavailable, or if there is a potential conflict of interest, **DON'T WAIT**! Report the incident to the Privacy Coordinator at (410-293-1550) or email: *privacy@usna.edu.* For more information on reporting privacy incidents, view USNA's Privacy Office Site: *www.usna.edu/AdminSupport/Privacy*.

For More Information

For more detailed guidelines on the safe handling of Sensitive PII and other Privacy Program topics, visit the USNA's Privacy Site at: *www.usna.edu/AdminSupport/Privacy*.