SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

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

What is PII?

PII is ANY information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as information found on a business card or official email signature block. This type of non-sensitive PII generally does not require special handling. There is also Sensitive PII, which if lost, compromised, or inappropriately disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII has stricter handling requirements, which are detailed below.

Examples of Sensitive PII include: Social Security numbers (SSNs), Tribal Enrollment Numbers, financial account numbers, date of birth, and biometric identifiers (e.g., fingerprint, facial image). Other data elements such as citizenship or immigration status, account passwords, and medical information[1], in conjunction with the identity of an individual, are also considered Sensitive PII.

The context of the PII should be considered to determine its sensitivity, such as a list of employees with poor performance ratings as opposed to a list of employees who completed privacy training. Note that even when an individual's name is not present it may still be PII if it can be used to identify or be linked to an individual, and PII can also be created when information about an individual is made available or combined with other information.

Collecting and Accessing Sensitive PII

Before collecting 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) the database or information technology system has an approved Privacy Impact Assessment. Access to Sensitive PII is based upon an official need to know, i.e., when the information relates to your official duties. Even if you are authorized to access PII, you should only access the PII you need to do your job. Privacy requirements apply to DOI contractors, and appropriate Federal Acquisition Regulations clauses and privacy provisions must be included in contracts to address privacy and security controls and safeguard PII.

Accessing PII during Telework: It is important that you understand DOI policy and guidelines for proper use and handling of Sensitive PII while teleworking. Review the DOI Telework Handbook and consult your supervisor to obtain approval and to discuss privacy considerations before removing PII from the workplace. When approved for telework and with supervisor approval, you are allowed to access, use, or send information while offsite for telework; however, you must apply appropriate protections to Sensitive PII at all times. Employees in a telework status are responsible for complying with all privacy requirements to secure the Sensitive PII they handle, just as they are while working at their official duty station. Discuss equipment, encryption, locking file cabinets and other safeguards with your supervisor to ensure you are equipped to protect Sensitive PII.

[1] Medical information that is not considered protected health information (PHI) subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Safeguarding Sensitive PII

Safeguard privacy at work: Always use your official DOI email account to transmit encrypted PII electronically – do not use personal email accounts to transmit or telework with Sensitive PII. Never take Sensitive PII home without supervisor approval. Ensure that 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 (press Ctrl + Alt + Delete at the same time, then select Lock Computer). Protect privacy while having intra-office or telephone conversations regarding Sensitive PII. Be alert to attempts to access or obtain PII, and immediately report suspicious activity to your supervisor or Bureau Privacy Officer.

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 authorized persons with an official need to know, and place the DOI Privacy Act Warning Notice on filing cabinets, storage containers, or otherwise prominently post it in areas containing PII. When faxing Sensitive PII is necessary, make sure the recipient is standing by to retrieve the fax and to provide confirmation to you that they received the fax.

Secure DOI media: Sensitive PII may only be saved, stored, or hosted on DOI-approved portable electronic devices (PEDs), such as laptops, USB flash drives, and external hard drives. All portable media must be encrypted pursuant to DOI policy and NIST standards. 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. 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).

Limit duplication of Sensitive PII: Carefully consider the need before creating new spreadsheets or databases that contain Sensitive PII from a larger file or database, and when it is necessary, make sure only the minimum data needed is used, that there are no hidden columns of data, and that Sensitive PII is safeguarded with the appropriate level of security controls.

Online Privacy

Do not post Sensitive PII on the DOI Internet, Intranet, shared drives, SharePoint, or multi-access calendars accessible to individuals without an official need to know or proper authorization. Always use appropriate controls to limit access to authorized users. Never post entries containing Sensitive PII on Facebook, Twitter, or any other social media application unless you have proper authorization.

Mailing Sensitive PII

Within DOI: Mail Sensitive PII in an approved messenger envelope provided by your office or mailroom. Be sure to encrypt Sensitive PII transmitted on CDs, USB flash drives, or other storage devices prior to mailing.

External Mail: Seal Sensitive PII in an envelope, and double wrap contents and tape both ends of the envelope; mark the inner envelope with appropriate markings and warning labels; be specific about the recipient so mail room or administrative personnel don't need to open it to find out who to route it to. Use First Class or Certified Mail, or a traceable commercial delivery service (e.g., UPS or FedEx). Encrypt Sensitive PII stored on CDs, DVDs, hard drives, USB flash drives, and other storage devices prior to mailing. Be sure to send passwords separately and a*lways verify that the recipient received the information.* Note that this only applies to Sensitive PII, other types of sensitive information may have additional handling requirements.

Emailing Sensitive PII

Outside DOI: When emailing Sensitive PII outside the DOI network, you **must** encrypt any attachment that contains Sensitive PII and provide the password separately to the recipient by phone or in person. Do not include Sensitive PII in the main body of the email, and always confirm that you have the correct email address and ensure the recipient is authorized to access and view the Sensitive PII.

Within DOI: PII may be emailed to a recipient with an official need to know within the DOI network as it is properly encrypted in the DOI environment. However, unencrypted PII creates a risk of unauthorized disclosure, especially when employees use the auto forward feature, reply to all, or forward to unintended recipients. As a best practice, you may remove or encrypt Sensitive PII you email within DOI to protect Sensitive PII and mitigate the risk of a privacy incident. Before emailing Sensitive PII within the DOI network, confirm that you have the correct email address – and always ensure the recipient is authorized to view the Sensitive PII.

Never Use Personal Email Accounts to Transmit Sensitive PII

Personal email accounts may not be used to transmit Sensitive PII. Sensitive PII may only be transmitted via official DOI email accounts. Personally-owned computers may not be used to access, save, store, or host Sensitive PII. Each bureau/office has different procedures for accessing the DOI network remotely, so check with your IT Help Desk.

Sharing Sensitive PII

You are authorized to share PII with authorized personnel within the agency for official purposes. You may share PII *outside* of DOI only if you have informed written consent from the subject individual, if the sharing is pursuant to one of the Privacy Act exceptions, or if the disclosure is in accordance with a published routine use in the applicable SORN.

Note that a "disclosure" of information can be by any means of communication – written, oral, or electronic. Any disclosure of information from a Privacy Act system to an external third party, including other Federal agencies, requires an accounting of the disclosure. This requirement does not apply to internal disclosures within DOI or those required by the Freedom of Information Act (FOIA). DOI personnel should use DI-3710 Disclosure Accounting Form to record disclosures to third parties.

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:

- Shred paper containing Sensitive PII using an approved cross-cut shredder[2]; do not recycle or place PII 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 IT Help Desk to sanitize Sensitive PII from computer drives and other electronic storage devices according to your bureau or office information security standards.
- Dispose of Privacy Act records by shredding or erasing in accordance with 383 Departmental Manual (DM) 8 and 384 DM 1. Disposing of documents in the regular trash or in recycling bins places the document at risk of unauthorized disclosure.

[2] See NIST SP 800-88 Revision 1 at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf for shredder requirements.

Reporting Privacy Incidents

A privacy incident is the loss of control, compromise, unauthorized disclosure or unauthorized access to PII, whether physical or electronic, and includes both suspected and confirmed incidents. It is every employee's responsibility to take appropriate action when an incident occurs.

Report Privacy Incidents Immediately

You must **immediately** report all suspected or confirmed privacy incidents, whether electronic or paper format, involving the loss or compromise of PII to your supervisor or Bureau Privacy Officer. If you can't reach them, you must immediately report the incident to the DOI Computer Incident Response Center (DOI CIRC) at (703) 648-5655 or DOICIRC@ios.doi.gov.

Be prepared to provide the following details:

- Date, time, and location of the incident
- Parties involved or affected
- Description of parties if unknown
- Violation description
- Do **not** contact the media (e.g., radio, TV, newspapers)
- If a crime is involved, report it to law enforcement or dial 911

Examples of privacy incidents include the following:

- Lost or stolen equipment– includes laptops, mobile phones, data storage devices, etc.
- Unencrypted transmission of PII – includes email, instant messages, internet and intranet postings
- Forgotten or missing files – includes files left on a desk, left in printer, copier or fax, lost or misfiled
- Improper disposal of PII – use an approved cross-cut shredder not a recycle bin, and never dispose of PII in trash bins
- Mailing PII – address should include complete and accurate address of recipient, and consider using encrypted media rather than hard-copy paper, especially if significant amounts of PII are involved
- Unattended privacy information – a box of PII files in the hallway or an unused and unsecured area
- Accessing or sharing PII with people who do not have an official need to know

See the DOI Privacy Loss Mitigation Strategy (PLMS) for detailed guidance on responding to a privacy incident.

Privacy Resources

Departmental Privacy Office:
DOI_Privacy@ios.doi.gov or 202-208-1605

DOI Privacy Program website:
http://www.doi.gov/ocio/information_assurance/privacy/index.cfm

Bureau/Office Privacy Officer contact information:
http://www.doi.gov/ocio/information_assurance/privacy/privacy-policy-contacts.cfm

Additional privacy resources are available on the DOI Privacy Portal:
https://portal.doi.net/CIO/IAD/ORG/privacy/default.aspx