



## HOW TO SAFEGUARD PERSONALLY IDENTIFIABLE INFORMATION

This factsheet is intended to help you safeguard **Personally Identifiable Information (PII)** in paper and electronic form during your everyday work activities. DHS employees, contractors, consultants, and detailees are required by law to properly collect, access, use, share, and dispose of PII in order to protect the privacy of individuals.

### 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 that found on a business card. Other PII is **Sensitive PII**, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. **Sensitive PII requires stricter handling guidelines.**

**Examples of Sensitive PII include:** Social Security number (SSN), alien registration number (A-Number), or biometric identifier (e.g., fingerprint, iris scan). Other data elements such as a driver's license number, financial information, citizenship or immigration status, or medical information, in conjunction with the identity of an individual, are also considered Sensitive PII. In addition, the context of the PII may determine its sensitivity, such as a list of employees with poor performance ratings.

### General Rules for Safeguarding Sensitive PII

A privacy incident is defined as the actual or potential loss of control, compromise, unauthorized disclosure, unauthorized acquisition or access to Sensitive PII, in physical or electronic form. Privacy incidents occur primarily when employees fail to use appropriate controls while accessing, using or sharing Sensitive PII or when they use Sensitive PII for an unauthorized purpose. The proper controls to safeguard Sensitive PII are detailed below.

### Collecting and Accessing Sensitive PII

If you are collecting or maintaining Sensitive PII electronically, be sure your database or information technology system has an approved Privacy Impact Assessment. Also, before collecting Sensitive PII, be sure that you have the authority to do so based on either the Privacy Act System of Records Notice (SORN) or a Standard Operating Procedure (SOP). Access to Sensitive PII is based upon your having a "need to know," i.e., when the information relates to your official duties. Limit your access to only that Sensitive PII needed to do your job, and do not view or use Sensitive PII for any purpose other than to do your job.

- Ensure documents are not accessible to casual visitors, passersby, or other individuals within the office without a "need to know." If you leave your work area for any reason, activate your computer's screen saver. At the end of your shift, either log off or activate a password-protected lock on your computer.
- Ensure privacy while having intra-office or telephone conversations regarding Sensitive PII.

### Using and Sharing Sensitive PII

You are authorized to share PII *outside* of DHS only if there is a published routine use in the applicable SORN and an information sharing and access agreement that applies to the information.

#### 1. **Proper use of email to share Sensitive PII:**

- a. **Sending Sensitive PII within or outside of DHS.** When emailing Sensitive PII outside of DHS, save it in a separate document and password-protect or encrypt it. Send the encrypted document as an email attachment and provide the password to the recipient in a separate email or by phone. [See the instructions in the *Handbook for Safeguarding Sensitive PII*.] Some components require encryption when emailing Sensitive PII *within* DHS, so check your policy.
- b. **Never email Sensitive PII to a personal email account.** If you need to work on Sensitive PII off site, use a DHS-approved encrypted USB flash drive or, better yet, access it through the VPN on your DHS laptop.

2. **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 at all possible.
3. **Proper use of the U.S. mail to share Sensitive PII:** Encrypt Sensitive PII stored on CDs, DVDs, hard drives, USB flash drives, floppy disks, or other removable media prior to mailing or sharing. *Note:* FOIA requests may require different handling instructions.
  - a. **Within DHS:** Sensitive PII should be mailed in blue messenger envelopes furnished by your onsite DHS mailroom or courier. Verify that the recipient received the information.
  - b. **External mail:** Seal Sensitive PII in an opaque envelope or container, and mail using First Class or Priority Mail, or a traceable commercial delivery service (e.g., UPS or FedEx).
4. **Safeguard DHS media:** Sensitive PII may only be saved, stored, or hosted on DHS-approved portable electronic devices (PEDs), such as laptops, USB flash drives, and external hard drives, all of which must be encrypted as noted in *DHS Sensitive Systems Policy Directive 4300A*. Personally-owned computers or USB flash drives may not be used. *Note:* If you need to transport your laptop or PED and must leave it in a car, lock it in the trunk so that it is out of sight. Do not leave your laptop or PED in a car overnight. If it is stolen or lost, report it as a lost asset following your component reporting procedures.
5. **Making electronic copies of Sensitive PII:** In some instances, it may be appropriate to create new spreadsheets or databases that contain Sensitive PII from a larger file or database. Before doing so, however, please consult Attachment S1 to the *DHS Sensitive Systems Policy Directive 4300A*.
6. **Posting Sensitive PII to web sites and shared drives:** Do not post Sensitive PII on the DHS intranet, the Internet (including social networking sites), shared drives, or multi-access calendars that can be accessed by individuals who do not have a “need to know.”
7. **Social engineering/phishing:** Be alert to any phone calls or emails from individuals claiming to be DHS employees and attempting to get personal or non-public information or asking to verify such information about you. DHS will not ask you to verify or confirm your account login, password, or personal information by email or over the phone.
8. **Sharing account logins and/or passwords:** Do not share account information, especially logins or passwords, with anyone. Do not have login or password information accessible to others (e.g., on a sticky note on your computer).

## Disposition 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; 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 according to your component’s information security standards or *DHS 4300A Sensitive Systems Handbook*.

## Report Privacy Incidents

You must report all privacy incidents, whether suspected or confirmed, to your supervisor immediately. If your supervisor is unavailable, or if there is a potential conflict of interest, report the incident to your Program Manager, Help Desk, component privacy officer or privacy point of contact. To obtain more information on privacy incident reporting, download the *Privacy Incident Handling Guidance* on DHS Connect.

## For More Information

To obtain more detailed guidelines on the safe handling of Sensitive PII, download the *Handbook for Safeguarding Sensitive PII* on DHS Connect, or email [privacy@dhs.gov](mailto:privacy@dhs.gov) to request a copy.

MAY 2011