Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

PII
HANDLE
WITH CARE

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. DHS employees, contractors, consultants, interns, and detailees are required by law and DHS policy to properly collect, access, use, safeguard, 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, which are detailed below***.
Examples of Sensitive PII include: Social Security numbers (SSN), Alien Registration Numbers (A-number), financial account numbers, and biometric identifiers (e.g., fingerprint, iris scan). Other data elements such as citizenship or immigration status, account passwords, and medical information, in conjunction with the identity of an individual, are also considered Sensitive PII. The context of the PII may also determine its sensitivity, such as a list of employees with poor performance ratings.

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, activate your computer's screen saver.
- Ensure privacy while having intra-office or telephone conversations regarding Sensitive PII.
- Do not post Sensitive PII on the DHS 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 DHS employees attempting to gather or verify personal or non-public information. DHS 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 *DHS Sensitive Systems Policy Directive 4300A*, Attachment S1.

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 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 portable media must be encrypted pursuant to *DHS Sensitive Systems Policy Directive 4300A*. Personal computers may not be used *unless you log in through the DHS Virtual Desktop*. 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 according to your component's reporting procedures.

III. 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.

Emailing Sensitive PII

- **Within DHS:** Though DHS policy allows you to email Sensitive PII without protection to a recipient with an official need to know, some components do require encryption. The DHS Privacy Office strongly recommends that you redact, password-protect, or encrypt Sensitive PII you email within DHS.
- **Outside DHS:** Email Sensitive PII within an encrypted attachment with the password provided separately by phone, email, or in person. 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 *unless you log in through the DHS Virtual Desktop*. Each component has different procedures for accessing the DHS network remotely, so check with your Help Desk.

Mailing Sensitive PII

Encrypt Sensitive PII stored on CDs, DVDs, hard drives, USB flash drives, floppy disks, and other removable media prior to mailing or sharing. *Always verify that the recipient received the information.* Note that FOIA requests may require different handling.

- **Within DHS:** Mail Sensitive PII in a blue messenger envelope provided by your on-site DHS mailroom or courier.
- **External Mail:** Seal Sensitive PII in an opaque envelope or container. Use First Class Mail, Priority Mail, or a traceable commercial delivery service (UPS, FedEx).

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:

- 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 and the *DHS 4300A Sensitive Systems Handbook*.

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. If your supervisor is unavailable, or if there is a potential conflict of interest, DON'T WAIT! Report the incident to your Program Manager, Help Desk, component privacy officer or privacy point of contact. For more information on reporting privacy incidents, download the *Privacy Incident Handling Guidance* on DHS Connect or www.dhs.gov/privacy.

For More Information

For more detailed guidelines on the safe handling of Sensitive PII, download the *Handbook for Safeguarding Sensitive PII* from www.dhs.gov/privacy.