# Handbook for Safeguarding Sensitive Personally Identifiable Information

March 2012

Homeland Security

*March 2012*

Dear Colleagues,

I am pleased to share with you the newly revised edition of the DHS Privacy Office's *Handbook for Safeguarding Sensitive PII* (Handbook) which applies to every DHS employee, contractor, detailee, intern and consultant.

This Handbook provides guidelines to help you safeguard Sensitive **Personally Identifiable Information (PII)** in both paper and electronic form at DHS. Your component Privacy Officer, component Privacy Point of Contact (PPOC), Program Office, or System Owner may set additional or more specific rules for handling PII, particularly *Sensitive* PII, based on the sensitivity of the information involved.

The Handbook provides step-by-step guidance on how to identify and protect Sensitive PII:

- In the office, or while traveling or teleworking
- On a portable electronic device, such as a Blackberry, laptop, or USB flash drive
- When emailing, faxing, or by other electronic transfer
- When mailing externally, overseas and inter-office
- When storing on a shared drive or SharePoint

The Handbook also provides simple instructions on:

- Encrypting Sensitive PII
- Securing Sensitive PII when not in use
- Disposing of Sensitive PII

By observing these guidelines, you will be doing your part to protect the Sensitive PII of our employees, contractors, and the public, and helping to prevent a privacy incident. If you have any questions regarding this Handbook, please contact your component Privacy Officer or PPOC. You may also call us at 703-235-0780 or email us at privacy@dhs.gov.

Sincerely,

Mary Ellen Callahan
Chief Privacy Officer
Chief Freedom of Information Act Officer
The Privacy Office
United States Department of Homeland Security

# Handbook for Safeguarding Sensitive PII

## Contents


Introduction....3
1.0 The Difference Between PII and Sensitive PII…. ....4
1.1 PII That Is Always Sensitive....5
1.2 PII That Is Sensitive In Certain Contexts ....6
1.3 Alien Files and Alien Numbers....6
2.0 Safeguarding Sensitive PII....7
2.1 Collect Sensitive PII Only as Authorized ....7
2.2 Limit Use of Sensitive PII....7
2.3 Minimize Proliferation of Sensitive PII ....8
2.4 Secure Sensitive PII ....9
3.0 Privacy Incident Reporting. ....11
3.1 How to Report a Privacy Incident....11
3.2 Do Not Further Compromise the Information ....11
Appendix A: Encrypting a File ....12
Appendix B: Frequently Asked Questions ....16
1. How can I protect Sensitive PII . ....16
A. *In the office?* ....16
B. *While traveling?*....17
C. *While teleworking?* ....17
D. *In email or other electronic transfer?*....18
E. *When sending via facsimile (fax)?* ....18
F. *In the interoffice mail?*....18
G. *In the outgoing mail?*....19
H. *When mailing overseas?* ....19
I. *On my office shared drive or SharePoint?* ....19
2. How can I minimize my use of Sensitive PII?....20
3. Why shouldn't I store Sensitive PII on unauthorized equipment? ....20
4. How do I secure Sensitive PII that cannot be encrypted?....20
5. What are my responsibilities when requesting or receiving Sensitive PII?....20
6. When and how should I destroy materials containing Sensitive PII?....21
Appendix C: Helpful Documents....22
Endnotes....23

# Introduction

As someone who works for or on behalf of the Department of Homeland Security (DHS or Department), it is your responsibility to protect information that has been entrusted to the Department. An important part of this duty is to ensure that you properly collect, access, use, share, and dispose of **Personally Identifiable Information (PII)**.

You should exercise care when handling all PII. *Sensitive* PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised.

This Handbook provides minimum standards that apply to every DHS employee, contractor, detailee, intern and consultant.[1] Your component Privacy Officer, Privacy Point of Contact (PPOC), Program Office, or System Owner may set additional or more specific rules for handling PII based on the sensitivity of the information involved. Your supervisor or component Privacy Officer or PPOC will be able to direct you to your component-specific rules.

This handbook explains:

- how to identify PII and Sensitive PII,
- how to protect Sensitive PII in different contexts and formats, and
- what to do if you believe Sensitive PII has been compromised.

Additionally, Appendix A of this handbook gives instructions on how to encrypt a file containing Sensitive PII. Appendix B provides answers to frequently asked questions on specific procedures for protecting Sensitive PII. And Appendix C includes three useful factsheets: one summarizing this handbook, one on protecting Sensitive PII while teleworking, and one providing instructions on how to restrict network shared drive access.

# 1.0 The difference between PII and Sensitive PII

DHS defines personal information as "**Personally Identifiable Information**" or PII, *which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.*

***Sensitive* PII** is *Personally Identifiable Information, 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 because of the increased risk to an individual if the data are compromised.

Some categories of PII are sensitive as stand-alone data elements. Examples include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. See the chart on the next page.

## 1.1 PII That Is Always Sensitive

| What is PII? | |
|---|---|
| **PII includes:** Name, email, home address, phone # | |
| **Sensitive PII includes:** | |
| ***If Stand-Alone:*** | ***If Paired With Another Identifier:*** |
| ➢Social Security number | ➢Citizenship or immigration status |
| ➢Driver's license or state ID # | ➢Medical information |
| ➢Passport number | ➢Ethnic or religious affiliation |

- Keep in mind that phone conversations are easily overheard between cubicles, so Sensitive PII is most securely discussed in an office or conference room behind a closed door.
- Remember that some places that seem private still pose a risk for unauthorized disclosure, such as in a taxicab or the DHS shuttle.

### B. While traveling?

- Sensitive PII should only be accessed via DHS-approved PEDs such as laptops, Blackberrys, 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 should not be used to access, save, store, or host Sensitive PII unless you log in through the DHS Virtual Desktop.* Each Component has a different procedure for accessing the DHS network remotely, so please check with your Help Desk.
- When transporting your laptop or PED:
  - If you must leave it in a car, lock it in the trunk so that it is out of sight. Do not le*ave your laptop or PED in a car overnight.*
  - Do not store a laptop or PED in an airport, a train or bus station, or any public locker.
  - Avoid leaving a laptop or PED in a hotel room. If you must leave it in a hotel room, lock it inside an in-room safe or a piece of luggage.
  - At airport security, place your laptop or PED on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on it until you can pick it up. Never place a PED in checked luggage.
  - If your PED is lost or stolen, report it as a lost asset following your component reporting procedures.

### C. While teleworking?

- Sensitive PII should only be accessed via DHS-approved PEDs such as laptops, Blackberrys, 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 should not be used to access, save, store, or host Sensitive PII unless you log in through the DHS Virtual Desktop.*
  - Each Component has a different procedure for accessing the DHS network remotely, so please check with your Help Desk.
  - Don't transfer files to your home computer or print agency records on your home printer.
  - Don't forward emails containing Sensitive PII to your personal email account (e.g., your Yahoo, Gmail, or AOL e-mail account) so that you can work on it on your home computer.
  - These rules also apply to all individuals on an approved telework program. [11]
- Obtain authorization from your supervisor to remove documents containing Sensitive PII from the office.

- Secure your PED and any hard copy Sensitive PII while teleworking, and ensure that other household members cannot access them.

*Consult Appendix C for more details on how to protect Sensitive PII while teleworking.*

## D. In email or other electronic transfer?

**Within DHS**: You can email Sensitive PII without protection if the recipient's need for the information is related to his or her official duties. However, if you have any doubt about that, or **to ensure protection**, the DHS Privacy Office strongly recommends that you password-protect Sensitive PII you email within the Department, or redact the Sensitive PII before you email or print it. Some components require encryption when emailing Sensitive PII *within* DHS, so check your component's policy.

**Outside of DHS**: Email the Sensitive PII within an encrypted attachment with the password provided separately (e.g., by phone, another email, or in person). See Appendix A for guidance on encryption techniques, and page 8 for guidelines on external sharing of Sensitive PII.

## E. When sending via facsimile (fax)?

- Avoid faxing Sensitive PII if at all possible. If you must use a fax to transmit Sensitive PII, use a secured fax line, if available. Alert the recipient prior to faxing so they can retrieve it as it is received by the machine. After sending the fax, verify that the recipient received the fax.

## F. In the interoffice mail?

- Sensitive PII should be sent in accordance with your Component's interoffice mail procedures,[12] or by DHS courier. Consult your supervisor for your office's accountable interoffice mail procedures. Verify that the recipient received the information.

### G. In the outgoing mail?

- For mailings containing a small amount of Sensitive PII materials (such as individual employee actions):
  - Seal Sensitive PII materials in an opaque envelope or container.
  - Mail Sensitive PII materials using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service (e.g., UPS).
- For large data extracts, database transfers, backup tape transfers, or similar collections of Sensitive PII:
  - Encrypt the data (if possible) and use a receipted delivery service (i.e., Return Receipt, Certified or Registered mail) or a tracking service (e.g., "Track & Return") to ensure secure delivery is made to the appropriate recipient.

### H. When mailing overseas?

- When serviced by a military postal facility (e.g., Army Post Office/Fleet Post Office), send Sensitive PII materials directly to the office via the U.S. Postal Service's First Class Mail.
- Where the overseas office is not serviced by a military postal facility, send the Sensitive PII materials through the Department of State diplomatic courier.

### I. On my office shared drive, SharePoint site, intranet, or public websites?

- Do not post Sensitive PII on the DHS intranet, component intranet sites, SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know."
- See Appendix C for the process to control access to a network shared drive, or consult your component Help Desk for assistance.
- For SharePoint collaboration site use, please consult the DHS/ALL/Privacy Impact Assessment (PIA)-037 found at www.dhs.gov/privacy. This PIA sets out minimum standards for SharePoint privacy and security requirements. DHS components may build more detailed controls and technical enhancements into their respective sites, so please contact your component Privacy Officer before establishing a new collaboration site that will contain PII.

## 2. How can I minimize my use of Sensitive PII?

Whenever possible, minimize the duplication and dissemination of electronic files and papers containing Sensitive PII.

- If you need to use a unique number or data element to identify individuals, use email addresses or case record numbers instead of Social Security numbers.
- Only print, extract, or copy Sensitive PII when the risk is justified by an official need that is not easily met using other means.
    - For example, if you need to generate a list of employees and their salaries in a particular office for a project, query the payroll database to return only those employees' names and salaries (and not, for example, other sensitive data such as SSNs). If you cannot customize the reports generated by a database, consider loading the results into an Excel spreadsheet and deleting the data you do not need before saving the file and distributing it to others. For more information, consult Attachment S1 in the *DHS Sensitive Systems Policy Directive 4300A: DHS Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII*, which can be found on DHS Connect.
    - Before emailing, printing or making paper copies, redact Sensitive PII that is not necessary for your immediate use or for a recipient to see.

## 3. Why shouldn't I store Sensitive PII on unauthorized equipment?

- DHS issued or approved PEDs such as laptops, Blackberrys, USB flash drives, and external hard drives, are encrypted.[13] Encryption protects the data on the device from being accessed by an unauthorized user if the device is lost or stolen.
- Non-government issued equipment, even if encrypted, may have unauthorized software or allow an unauthorized person to access the data. This equipment may also have viruses, spyware, or other technology that may cause harm to the DHS network, and could allow unauthorized access to DHS information, including Sensitive PII, if the non-government issued equipment is connected to the DHS network.

## 4. How do I secure Sensitive PII that cannot be encrypted, such as paper copies or some external media?

- Sensitive PII in hard copy or stored on external media must be kept in a locked compartment, such as filing cabinet or desk drawer. Alternatively, hard copies can be scanned and password protected or encrypted. External media can be mailed using the instructions outlined in this document.

## 5. What are my responsibilities when requesting or receiving Sensitive PII?

When collecting Sensitive PII from members of the public, use only an OMB-approved[14] paper or electronic form, and collect Sensitive PII directly from the individual to the extent possible.

- For example, if a DHS employee needs to submit information about a visitor to have him or her cleared to enter a DHS facility, the *visitor* should fill out his or her portion of the approved visitor form whenever possible.[15] This will limit unnecessary dissemination of that individual's personal data, and will also allow him or her to be aware of what information is being collected, to consent to releasing that information, and to receive notice as required by the Privacy Act of the uses and purpose for collecting the information.
- As a best practice, every request you make for Sensitive PII should be accompanied by a reminder of how to properly secure the information. DHS suggests the following reminder when requesting information from someone outside of DHS:

  *"The information I have requested is Sensitive Personally Identifiable Information. To properly secure this information, please send it within an encrypted and password-protected attachment with the password provided under a separate cover, such as in person, by phone, or in a separate email."*

- If someone sends you Sensitive PII in an unprotected manner, you must protect that data in the same manner as all Sensitive PII you handle once you receive it.
  - For example, if someone outside of DHS sends unsecured Sensitive PII in the body of an email to you, you must encrypt that data if you wish to email it to another non-DHS recipient.
  - The DHS Privacy Office strongly recommends that you password-protect Sensitive PII you share within the Department, or redact the Sensitive PII before you share or print it.

## 6. When and how should I destroy materials containing Sensitive PII?

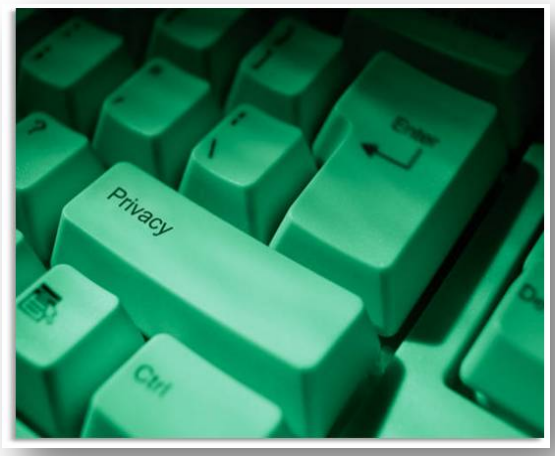
Follow retention and disposal policies: Sensitive PII, including archived emails[16] containing Sensitive PII, shall be destroyed when retention of the data is no longer required, consistent with applicable record retention schedules[17] or as identified in the applicable SORN or PIA published on www.dhs.gov/privacy.

- Printed material must destroyed using an approved shredder or "burn bag." Secure burn bags containing Sensitive PII that are awaiting removal.
- All Sensitive PII on diskettes must be permanently erased or destroyed according to your ISSM's standards before re-use.
- PEDs containing Sensitive PII must be sanitized according to your ISSM's standards when no longer needed by an employee or contractor.

# Appendix C: Helpful Documents

At the end of this document you will find three helpful factsheets:

1. ***How to Safeguard Sensitive Personally Identifiable Information***: summarizes the key points in this Handbook.
2. ***Protecting PII: Telework Best Practices***: details the steps to protect Sensitive PII while working remotely.
3. ***Controlling Access to a Network Shared Drive Folder***: details the steps to restrict access to a particular folder within your shared drive that may contain Sensitive PII.



# Endnotes

[1] As required by OMB M-07-16, these rules also apply to DHS licensees, certificate holders, and grantees that handle or collect PII, including Sensitive PII, for or on behalf of DHS.
[2] Subsection (e)(10) of the Privacy Act of 1974, as amended (5 USC § 552a) states that "[e]ach agency that maintains a system of records shall…establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."
[3] For more information about the Paperwork Reduction Act (PRA) (44 U.S.C. 3501 et seq.), contact the DHS PRA Program Office at DHSPRA@hq.dhs.gov.
[4] DHS Management Directive 11042.1: *Safeguarding Sensitive But Unclassified (For Official Use Only) Information* defines need to know as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized Governmental function, i.e., access is required for the performance of official duties.
[5] Depending on your role in the Department, the appropriate supervisor may be your Program Manager, Director, Privacy Officer, or ISSM. You are also encouraged to contact the DHS Privacy Office at privacy@dhs.gov if you need assistance locating the person who can respond to your privacy questions, have privacy issues that need escalation, clarification, or resolution, or if you need your concern to be kept confidential. Also, you should refer to the DHS Office of Inspector General (OIG) any alleged violations of the terms of this document that may constitute criminal misconduct, identity theft, or other serious misconduct, or reflect systemic violations within the department. You can contact the OIG by writing to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528. You can also fax the information to (202) 254-4292, or email DHSOIGHotline@dhs.gov.
[6] NDAs are generally obtained from DHS contractors prior to those individuals being issued a badge and/or access to DHS systems, as part of the security on boarding process.
[7] If you are unsure to whom to refer the request, contact your supervisor or the FOIA office at FOIA@dhs.gov.
[8] DHS Sensitive Systems Policy Directive 4300A, section 4.8.3 (b) states that "equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component ISSM."
[9] DHS Management Directive 3070.2, *Telework Directive*, specifies that "[t]eleworking employees are subject to ensuring that records subject to Privacy Act and sensitive or classified data are not disclosed to anyone except those who are authorized access to such information in order to perform their duties."
[14] To obtain more information on privacy incident reporting, download the *Privacy Incident Handling Guidance* at www.dhs.gov/privacy.
[11] DHS Management Directive 3070.2, *Telework Directive*, specifies that "[t]eleworking employees are subject to ensuring that records subject to Privacy Act and sensitive or classified data are not disclosed to anyone except those who are authorized access to such information in order to perform their duties."
[12] For more information on accountable interoffice mail, see the *Outgoing Mail Policies and Services* section of the DHS Executive Secretariat Handbook or contact the DHS mailroom. If your office does not participate in DHS HQ interoffice mail, consult your supervisor for your local accountable interoffice mail procedures.
[13] OMB Memorandum M-06-16 requires that all agencies "[e]ncrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing." Encryption of all mobile computing devices is required by *DHS Sensitive Systems Policy Directive 4300A*. If you are issued a portable electronic device which you believe may not be encrypted, contact your component ISSM.
[14] See OMB Office Of Information And Regulatory Affairs *Inventory Of Approved Information Collections* at www.whitehouse.gov/omb for a list of OMB-approved forms.
[15] Subsection (e)(2) of the Privacy Act of 1974, as amended (5 USC § 552a) states that "[e]ach agency that maintains a system of records shall…collect information to the greatest extent practicable directly from the

subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."

[16] Archived emails in this context include only those that the user manages, not those saved as part of system backups by system administrators.

[17] For questions about record retention schedules, contact your Component Records Officer or DHSRecordsManagement@HQ.DHS.GOV.

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

# 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.

# Protecting PII: Telework Best Practices

## Teleworking and Information Security

Telework presents many benefits to the federal workforce, such as managing commutes, saving taxpayer money by decreasing government real estate, and ensuring continuity of essential government functions in the event of emergencies. While telework allows for greater flexibility in managing our workforce, there are risks to privacy and information security[1] that are inherent with a remote workforce. Information security policies do not change when an employee works from home. It is the duty of the employee to safeguard Sensitive information, including personally identifiable information (PII),[2] while teleworking.

## Safeguarding Sensitive PII

Effective teleworking begins with having a signed telework agreement in place. Work with your supervisor to determine what types of documents are appropriate to take home and what documents should stay secured within the DHS work space. Know the sensitivity of your documents, and make sure they are appropriately marked to help mitigate the risk of unauthorized disclosure.

One of the most effective ways to safeguard documents containing Sensitive PII is to keep electronic documents within the DHS network and to properly secure hard copy documents that you take outside of the DHS work space. Stay within the network by logging in remotely through the DHS Virtual Desktop*, whether you use your DHS-issued laptop or your personal computer. If you choose to work from your personal computer, **do not forward documents to your personal email account** as a way to avoid issues such as slow network connectivity or the inability to print. While there may be instances where you need to send information to an individual's personal account (i.e. job applicant), forwarding unencrypted emails to your own personal email account or sending unencrypted documents outside the DHS network that contain Sensitive PII is considered a privacy incident (or data breach).

If you know you will be teleworking, identify the files you may need to work on in advance, and organize them on your network drive or DHS laptop so that they will be easily accessible to you while teleworking. You may also want to take advantage of DHS-approved collaboration tools, such as SharePoint, to easily access files while teleworking. However, before using SharePoint to store Sensitive PII, make sure your site has been approved for such use and that access is limited to only those individuals whose need for the information is related to his or her official duties. Have a back-up plan in mind in case you experience issues with network connectivity, but never transfer files to your personal computer using thumb drives or other portable electronic devices.

Be able to secure your DHS equipment and information at all times, including while transporting information home or while traveling. If you must leave equipment or documents unattended, secure them (i.e. in the trunk of your car, in a hotel safe, etc.), but only for short periods of time. Inventory your documents before teleworking, and ensure all documents are returned to the office.

## Examples of Privacy Incidents Associated with Telework

Know how to recognize a privacy incident and how to report it.

- Sending an email containing Sensitive PII to your personal email account.
- Sending unencrypted Sensitive PII outside the DHS network (i.e., to another agency, to a private sector partner, to a potential hire).
- Allowing family members access to documents containing Sensitive PII.
- Printing documents containing Sensitive PII to your personal printer.
- Using a thumb drive or other device to transfer data (i.e., Sensitive PII) to your personal computer.

***Report any suspected or confirmed privacy incidents to your supervisor or your component Help Desk.***

[1] The Federal Information Security Management Act of 2002 (FISMA) defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

[2] PII is any information that can directly or indirectly lead to the identification of an individual. Sensitive PII is defined as personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

**March 2012**

| WHEN | DO | DON'T | WHY |
|---|---|---|---|
| Before you telework… | ✓ **Plan ahead to ensure that Sensitive documents can be safely accessed remotely.** Organize your files so that they are easily accessible via the DHS Virtual Desktop*. Use DHS-approved, portable electronic devices, which are encrypted, thereby adding a layer of protection to your data. | ✗ **Don't forward emails to your personal email account or use non-approved portable electronic devices.** Have a back-up plan in case you experience issues with network connectivity, but never transfer or download data to your personal computer, personal email account, or to non-encrypted devices. | When you remove data from the DHS network, DHS cannot protect it. There may be instances where you need to send Sensitive PII to job applicants or individuals without DHS accounts, but it must be encrypted. To send it unencrypted is considered a privacy incident. |
| | ✓ **Obtain authorization from your supervisor to take home Sensitive documents, and make sure documents containing Sensitive PII are marked "For Official Use Only" or "Privacy Data."** Inventory your hard copy documents when you leave the office and before you return them to the office. | ✗ **Don't take Sensitive PII home that you do not need.** Limit your removal of Sensitive PII from the office to only that information that is relevant and necessary to the work outlined in your telework agreement. | Hard copy documents are easily lost or misplaced, putting Sensitive PII at risk. Conducting an inventory and properly marking documents helps mitigate the risk of unauthorized disclosure. |
| Transport of documents … | ✓ **Be able to secure Sensitive data when not in use.** If you must leave your laptop or hard copy documents inside a vehicle, lock them in the trunk but only for short periods of time. When traveling, place Sensitive data in a hotel safe when not in use. | ✗ **Don't leave your laptop or hard copy documents unattended overnight.** Maintain accountability of your data by ensuring documents are secured when not in use. | Failure to maintain accountability of Sensitive PII can lead to loss, theft, or misuse, resulting in a privacy incident. |
| At home… | ✓ **Log in through the DHS Virtual Desktop*** Organize your work space at home so that work files are separate from personal files and can be properly safeguarded. | ✗ **Don't email or save files containing Sensitive PII to your home computer.** ✗ **Don't print agency records to your home printer.** | Your home computer, printer, fax, and copier all contain internal storage or "hard drives." Even when these devices are disposed of, the information stored within is vulnerable. |
| | ✓ **Take advantage of DHS collaboration tools such as SharePoint.** Do not post Sensitive PII on the DHS intranet, Component intranet sites, SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know." | ✗ **Don't store Sensitive PII on SharePoint unless your site has been approved for such use.** Access must be limited to those that have an official need to know. | Collaboration tools provide quick, easy access to data, but without proper security controls, can lead to data winding up in the wrong hands. Sharing Sensitive PII with unauthorized users is considered a privacy incident. |
| | ✓ **Secure your data, and ensure other household members do not have access to it.** Organize your work space at home so that government property and information are kept separate from personal property and can be properly safeguarded. | ✗ **Don't leave files containing Sensitive data lying out in the open.** Never leave Sensitive PII in view of children, spouses, or visitors. Sensitive PII should be secured in locked cabinets and your computer/Blackberry should remain locked when not in use. | Failure to properly secure Sensitive records could result in inadvertent sharing of Sensitive PII. |

*Each Component has a different process for accessing the DHS network remotely. Please contact your Help Desk.

**March 2012**

# Controlling Access to a Network Shared Drive Folder

*August 2011*

Most likely your office maintains space on a DHS shared network drive. Your office controls access to its portion of the shared drive through a folder-based security mechanism. Typically, access to your main folder is restricted to the staff on your office's main email distribution list.

If you want to restrict access to a particular folder within your shared drive, here's what to do:

1. Create/identify the folder you want to control.
2. Find the full path to that folder by:
    a. Clicking on My Computer on your desktop.
    b. Finding your network shared drive and right clicking it.
    c. In the left NAV under "Details", the network drive path will appear, for example:
        - \\ZZA1CE-0350\dhs-g\DHS\Your Office\Your Folder
3. Create the name of an email distribution list that you'd like to use to govern access to the folder. Use something like "officename [folder]". Keep it short, simple, easy to recognize in the GAL. This email list becomes your security group, and as the manager of this group, you have the ability to add and remove names of users, as needed. To do this [once the email list is created], open the security list in the GAL, click "modify members", then add or remove users.
4. Identify who you want to have access to that folder – you will need full DHS email addresses.
5. Email IT Support and tell them you want to:
    a. Restrict access to a folder. Send them the full path (step 2).
    b. Create an email distribution list with the names you picked (step 3); and
    c. Add all the names/email addresses to that distribution list and give each of those individuals "owner" rights to the distribution list – this way anyone in that list can change the list if you want to add/remove names. You can also pick one person and give them ownership rights to add/remove people from the distribution list. However you do it, it's key that someone you know can edit that list of names – this will give you control over who can access the folder.
    d. Restrict access to that folder so that only users on the distribution list can access it. You can make this a little more complex by changing the tiers of control over the folder.
        i. Full restriction/access – only those on the list can open the folder and once they're in they can do anything they want.
        ii. Read only – you can allow anyone to read files in that folder – they cannot edit/delete anything – then only people on the distribution list can change.
6. Then get confirmation from IT Support, and conduct a test –
    a. See if someone outside your new group can open the folder.
    b. See if someone inside your group can open the folder and change stuff in it.
    c. See if someone on your list can change the names on the list.