DHS

Publish Date: October 2024

Learning Technology & Innovation (LTI)

Division Transcript Content

Course Title:	**Privacy at DHS: Protecting Personal Information FY25**
Course ID	ET-35010:
Content ID	ProtectingPrivacy_051721.zip
Course Description	In our mission to secure the homeland, we need to collect personal information from citizens, legal residents and visitors, and we are obligated by law and DHS policy to protect this information to prevent identity theft or other adverse consequences of a privacy incident or misuse of data. This brief course is designed to raise your awareness of the importance of maintaining privacy in the workplace and will convey methods of safeguarding personal information.
Course Goal	Raise awareness and comprehension of protecting personal information in the workplace
Target Audience	All DHS Personnel

This course provides role-based training for handling personally identifiable information (PII) and sensitive PII (SPII) to DHS federal and contractor employees who will have access to PII and SPII.

OBJECTIVES:

At the end of this course, you should be able to:

- Define Personally Identifiable Information (PII)
- List the potential consequences of not protecting PII
- Discuss the required methods for collecting, using, sharing, and safeguarding PII, and
- Report any suspected or confirmed privacy incidents

Hi, I'm the DHS Privacy Man. For the next 15 to 20 minutes, I want to talk to you about the importance of safeguarding personal information, such as Social Security numbers, that DHS may collect or store in its databases or in paper files. Congress and OMB have mandated privacy training for both employees and contractors at all federal agencies to help staff identify and mitigate privacy risks related to sensitive personal information, which I will define in a moment.

In our mission to secure the homeland, DHS needs to collect, maintain, use, and disseminate personal information, also known as Personally Identifiable Information or PII, from citizens, legal residents, and visitors. DHS is obligated by law and DHS policy to protect this information to prevent identity theft or other adverse consequences of a privacy incident or misuse of data. As DHS staff who might collect, use, maintain, or disseminate PII, you need to:

1. Know how to protect PII; and
2. Report any suspected or confirmed privacy incidents.

Before we discuss your role in protecting privacy at DHS, let me tell you about the framework we use to assess privacy risks associated with any new technology at DHS that collects PII.

We use the DHS Fair Information Practice Principles, or FIPPs, as our framework for identifying and mitigating privacy risks. When new systems are developed or updated to collect, maintain, use, or disseminate PII, privacy staff in the Components meet with the project manager early in the design process to review the FIPPs as part of our compliance documentation process to:

1. Assess the need for, and scope of, any collection, maintenance, use, or dissemination of PII, and
2. Embed privacy protections in the Information Technology system at the front-end.

We ask the system development team questions like:

1. Is the PII you plan to collect, maintain, use, or disseminate relevant and necessary and
2. What is your purpose and authority to collect this information?

If you are a program manager or system owner, it is important to understand your responsibilities for completing privacy compliance documentation before your system becomes operational. Depending on the nature of your system or program, privacy compliance documentation such as a Privacy Impact Assessment, required by the E-Government Act of 2002, and/or a System of Records Notice, required by the Privacy Act of 1974, may be required.

Although this course will not get into the details of how to prepare these documents, it is important to recognize that privacy compliance gaps can put your system or program at risk. For example, a recent Government Accountability Office report recommended that the Chief Privacy Officer investigate whether a system should be suspended until privacy compliance documentation could be completed. We encourage program managers and system owners to consult with their Component Privacy Officer or Privacy Point of Contact early in the Systems Development Lifecycle to ensure that privacy requirements are addressed.

So, what do I mean when I refer to personal information?

At DHS we call personal information “personally identifiable information”, or PII:

DHS defines PII as 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, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII includes but is not limited to Social Security numbers, driver’s license numbers, Alien Registration numbers, financial or medical records, biometrics, or a criminal history. This data requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

PII and Sensitive PII as privacy incidents are not necessarily cut and dried. In some cases, PII that is not Sensitive would be reported as a privacy incident depending on context. For example, a loss of a contact list with the names of people who attended training would not be considered a privacy incident. However, if it is a list of employees who are being disciplined for not attending training and it is lost or compromised, then that would be considered a privacy incident. In this instance, it is the context of the information that would cause this to be a reportable privacy incident.

Also, the loss of Sensitive PII even in an encrypted or password-protected format could become a privacy incident. For instance, if encrypted or password-protected Sensitive PII, along with the "key" or password to access the information, is sent to a person without a "need to know" or to a personal e-mail address, this would be considered a privacy incident.

If you’re confused, stay with me and in a few minutes, I will walk you through specific examples on how you can safeguard Sensitive PII.

DHS Components collect a wide range of PII for reasons varying from national security to the distribution of disaster relief funds.

To give you a sense of the magnitude of the PII handled by DHS, every day we collect and safeguard PII on over 3 million domestic and international travelers. And that's just one example.

If we fail to protect PII, there can be severe consequences for everyone.

Most privacy incidents occur when employees mishandle PII due to a lack of awareness of PII safeguards, and when that occurs, they receive counseling and additional training.

But we have also experienced intentional privacy incidents at DHS. For example, a FEMA employee was sentenced to 5 years in prison for stealing the identities of more than 200 disaster survivors who had applied for government assistance.

If you:

- Lose, allow, or witness unauthorized access to Sensitive PII. Unintentionally release Sensitive PII.
- Misuse Sensitive PII.
- Cause files or systems to become compromised.
- Know or suspect that any of the above has occurred.

You MUST report the privacy incident, either suspected or confirmed, immediately to your supervisor, Component help desk, privacy officer, or privacy point of contact.

In this scenario, you will play the role of a FEMA employee who processes disaster assistance claims that contain Sensitive PII.

Privacy Man: You've just finished taking a much-deserved break and have returned to your workstation. It seems like you've been processing disaster assistance claims for months, when in reality it's only been three long days since the record-breaking flood hit the northeast.

Privacy Man: After you unlock your computer and continue working, someone approaches the entrance to your cube…

Katelyn Baker: Hello, you don't know me, but I am helping distribute disaster relief funds. Can you give me Polly Smith's Social Security number?

Collecting and Accessing Sensitive PII

In this case, what is the proper procedure for sharing Polly Smith's Sensitive PII?

a. Ask the employee for her identification and her reason for requesting Miss Smith's Sensitive PII.
b. Provide the employee with the information she requested.
c. Contact your supervisor immediately and let her know someone you've never met before is requesting Sensitive PII.
d. Tell the employee you will email it to her after you finish the claim you are working on.

Feedback

You chose option A. That's right! The proper procedure is to ask the requestor for her identification and her reason for requesting the PII. Access to PII must meet two requirements: (1) the requestor must have a need to know the information in their official capacity; and (2) if they are a non-DHS employee or contractor, the disclosure of PII must be authorized and in compliance with the Privacy Act of 1974. If you are unsure, please refer the requestor to your supervisor before disclosing any PII to persons who are not agency employees.

Privacy Man: You let the employee know that her ID badge was turned backwards, asked her to introduce herself and why she needs to know Miss Smith's Sensitive PII.

Katelyn Baker: Oh, I'm sorry. My name is Katelyn Baker, and I'm a contractor assigned to assist with the distribution of disaster relief funds. Polly Smith hasn't received her assistance funds yet. I need her Social Security number so I can check on the payout of her funds.

Privacy Man: You recognize Katelyn's name and heard that she and her employer have been doing a great job helping FEMA respond to the numerous claims that have been filed. You let Katelyn know that you are currently busy with another request but will email her Polly Smith's SSN later today.
Later that afternoon, you begin drafting the email to Katelyn when you remember that she is an outside contractor. You know that many privacy incidents are the result of poor email practices, so you need to send this Sensitive PII using the proper procedure.

Using and Sharing Sensitive PII

What is the proper method for emailing Sensitive PII outside of the Department?

a. Sensitive PII should not be sent outside of the Department via email.
b. Type the requested Sensitive PII into the body of the email and send the email. Follow-up with a phone call to the recipient to make sure they received the information.
c. Save the Sensitive PII in a protected file type, encrypt or password-protect the document, attach it to the email, and then follow up with either a phone call or a separate email containing the password to open the file.

Feedback

You chose option C. That's right! Be sure to consult the Handbook for Safeguarding Sensitive PII in the Resources section for specific instructions on how to encrypt or password protect a file.

It's important to note that some DHS components require email encryption or password protection for internal as well as external sharing of Sensitive PII. In some instances, it is appropriate to email Sensitive PII outside of the Department. However, it is never appropriate to email Sensitive PII to a personal email account for work-related purposes.

Privacy Man: After sending the email, you called Katelyn Baker to provide her with the password to access the files you just sent.

Katelyn Baker: Thank you so much for emailing me Miss Smith's information. The password works and I'm looking at her information now. While I have you on the phone, can I ask you to email me copies of the claim forms for the 20 claimants on Canal Street that we discussed? Sorry, but I forgot to ask you when I stopped by.

Privacy Man: You tried to email the 20 claim forms to Katelyn, but the files are too large to send via email. Your only other option is to mail the Sensitive PII to her. You know that mail often gets compromised while in transit, so it's a shame that you are not able to email the forms or else you could scan them and send password-protected versions to her.

Using and Sharing Sensitive PII

Since you can't email the claim forms to Katelyn's office, what is the preferred method for mailing Sensitive PII externally?

a. Scan the claim forms and save the data onto an encrypted CD. Seal it in an opaque envelope and mail it using First Class or Priority Mail, a courier, or a traceable commercial delivery service like UPS, the USPS, or FedEx.
b. Mail a hard copy of the claim forms using a traceable commercial delivery service like UPS, the USPS, or FedEx.

Feedback

You chose option A. That's right! You really want to avoid mailing anything that contains Sensitive PII, but if you have to, the preferred method is to:

1. Scan the hard copy Sensitive PII and save it onto an encrypted CD or other DHS-approved portable media.
2. Mail the portable media using First Class or Priority Mail, a courier, or a traceable commercial delivery service like UPS, the USPS, or FedEx.

You've completed Katelyn's request for PII and now it's 5 o'clock and time to head home.

But first, since you are working from home tomorrow, you need to pack your briefcase with everything you need, including some Sensitive PII.

Please consult the Handbook for Safeguarding Sensitive PII in the Resources to answer this question:

What is the best way to access Sensitive PII while away from the office?

a. Email the Sensitive PII, via a password-protected document, to your personal email account that you can access from home.

b. Pack hard copies of the Sensitive PII into your briefcase in a folder marked "Confidential."

c. Save Sensitive PII to, or access it from, an encrypted, DHS-approved portable electronic device.

Feedback

You chose option C. That's right! If you telework or travel for work, you need to follow these guidelines to safeguard Sensitive PII:

- Use DHS-approved portable electronic devices, which are encrypted.
- Get your supervisor's permission to remove hard copy Sensitive PII from the office.
- Secure all Sensitive PII when not in use.
- Log in through the DHS secured portal.
- Take advantage of collaboration tools such as SharePoint.

So, you've just learned how to prevent the 4 most common privacy incidents at DHS.

Allow me to reiterate the key points for you to remember, and highlight some new points:

Sharing Sensitive PII: It is important to protect Sensitive PII at all times. Share it only with people who have an official "need to know."

Emailing to the wrong recipient or personal accounts: Never email Sensitive PII to a personal email account. If you need to work on Sensitive PII off site, use a DHS-approved portable electronic device.
Preventing Compromised Mail: If documents can't be scanned and encrypted or password-protected, mail them in an opaque envelope or container using First Class, Priority Mail, or a traceable commercial delivery service like UPS, the USPS, or FedEx.

Accessing Sensitive PII while away from the office: The best method is to save the Sensitive PII on an encrypted, DHS-approved portable electronic device.

Lost Media: Do not leave any portable electronic devices in a car. If it is stolen or lost, report it as a lost asset following your component reporting procedures.

Lost Hard Copies: Secure Sensitive PII in a locked desk drawer or file cabinet. 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.

Posting Sensitive PII to websites 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 an official "need to know."

To promote privacy here at DHS, I encourage you to:

1. Partner with your Component Privacy Office when planning new or updating existing programs, systems, technologies or rule-makings to ensure compliance with privacy laws.
2. Follow the procedures outlined in the Handbook for Safeguarding Sensitive PII at DHS.
3. Report all suspected or confirmed privacy incidents immediately.

And when you work with Sensitive PII, be sure to consult the resources listed on the Privacy Resources section.

There are several resources you can reference when handling PII to make sure you are following the proper procedures:

• Privacy Office website: www.dhs.gov/topic/privacy

• Handbook for Safeguarding Sensitive PII (https://dhsconnect.dhs.gov/org/comp/cisa/privacy/Documents/DHS%20Handbook%20for%20Safeguarding%20SPII_Dec%202017.pdf).

Employee Acknowledgement Form

PERSONALLY IDENTIFIABLE INFORMATION (PII)
EMPLOYEE ACKNOWLEDGMENT AND AGREEMENT

Definitions of Personally Identifiable Information (PII) and Sensitive PII

Personally identifiable information (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 that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. See Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security, DHS Privacy Office.

Employee Acknowledgment and Agreement

I attest that I understand my responsibility to safeguard PII, including Sensitive PII; and, that I am familiar with and agree to comply with the standards for handling and protecting PII. I also agree to report the potential loss, theft, improper disclosure or compromise of PII. I acknowledge that I have received proper training regarding the procedures for safeguarding PII, and that I am aware of Department protocols should PII be potentially lost, stolen, improperly disclosed or compromised. I further understand that my failure to act in accordance with my responsibilities outlined above may result in criminal, civil, administrative, or disciplinary action if I am found responsible for an incident involving the loss, theft, unauthorized or improper disclosure or compromise of PII or Sensitive PII. Additionally, as a DHS employee, I am aware that I am subject to the policies contained within 5 CFR 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch and DHS MD 0480.1, Ethics/Standards of Conduct (January 1, 2010).

Privacy Resources

Handbook for Safeguarding Sensitive PII at DHS

https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information

Privacy Office website:

https://www.dhs.gov/topic/privacy

For privacy concerns, consult your Component's Privacy Officer or Privacy Point of Contact.

Please proceed to the next page for the Privacy at DHS: Protecting Personal Information Post Assessment

Post Assessment

Now that you have finished reviewing the course material, please complete the Post Assessment test questions on the following pages. Once complete, select the "**Submit Test**" button to view number of correct answers. If you have met the requirement for number of correct answers, the '**View Certificate**' button will display. You will be prompted to print the digitally signed certificate for your records. If you would like to retake the test at any point, select the "**Reset Test**" button to clear your existing selections and restart the Post Assessment test.

You need to correctly answer **7 out of 9** questions in order to pass the assessment and receive credit for completing the training.

1. A privacy incident is: the suspected or confirmed loss of control, compromise, unauthorized disclosure unauthorized acquisition, or any similar occurrence where:
    a. a person other than an authorized user accesses or potentially accesses PII; or
    b. an authorized user accesses or potentially accesses PII for an unauthorized purpose.

- ◯ True
- ◯ False

2. Indicate which of the following are examples of PII (check all that apply):

- ☐ A leave request with name, last 4 of SSN and medical info
- ☐ An employee roster with home address and phone number
- ☐ TSA's Standard Operating Procedure for airport screening
- ☐ A supervisor's list of employee performance ratings
- ☐ A witness protection list
- ☐ A worker's compensation form with name and medical info

3. If someone within DHS asks you for PII in digital or hard copy format, what should you do first?

- ◯ Verify the requestor's "need to know" before sharing
- ◯ Redact all your PII before you share it
- ◯ Deny the request
- ◯ All of the above

4. Who is responsible for protecting PII

- ◯ Component Privacy Officers
- ◯ Supervisors
- ◯ Contractors
- ◯ All of the above

5. Personally-owned equipment can be used to access or store PII for official purposes.

- ◯ True
- ◯ False

6. If you maintain PII in hard copy or electronically, use safeguards and technical access controls to restrict access to staff with an official "need to know."

- ◯ True
- ◯ False

7. Privacy Act protected information can be shared outside of DHS only when specifically authorized. (Note: Check with your Privacy Officer or Legal Counsel if you have any question about authority.)

- ◯ True
- ◯ False

8. Never email another individual's PII to or from your personal email account.

- ◯ True
- ◯ False

9. You may only email PII from DHS to an *external* email within an encrypted or password-protected attachment. (Note: We strongly recommend that you redact, password-protect, or encrypt PII emailed *Internally* to DHS, especially when emailing to distribution lists. Some Components require the exryption of PII emailed internally.

- ◯ True
- ◯ False

Number of correct Answers:

0

Correctly answer **7** out of **9** questions in order to pass

Submit Test **Reset Test**