Protecting Personally Identifiable Information

Audio is available only by conference call.

Please call: (800) 700-7784

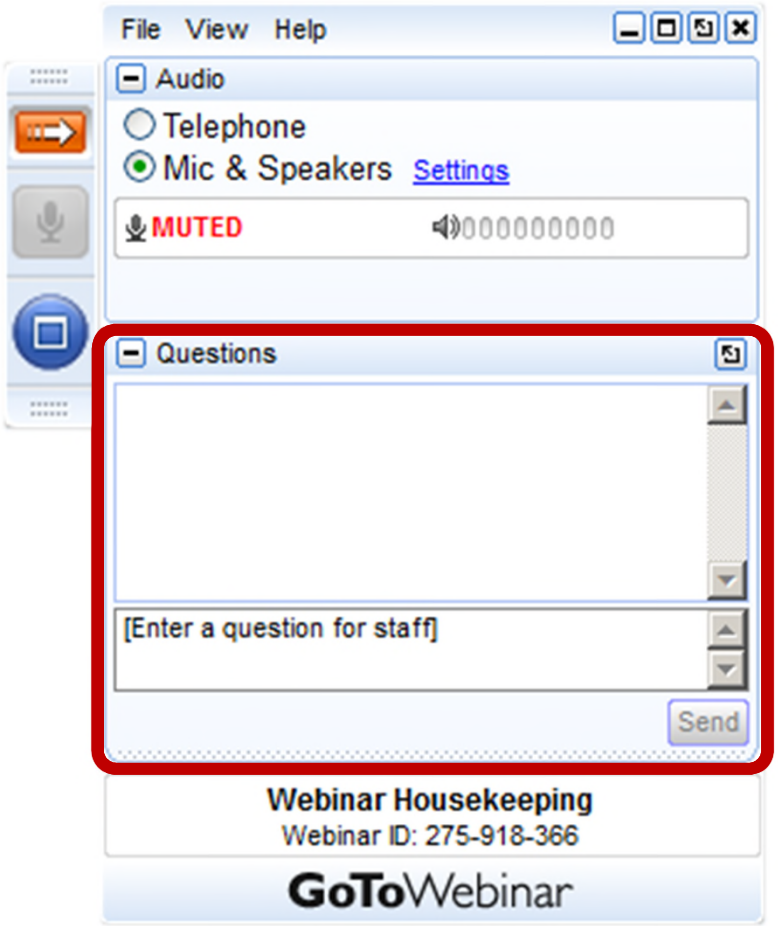
Participant Access Code: 365268

to join the conference call portion of the webinar

Webinar Logistics:

- Audio is being recorded. It will be available along with the PowerPoint at www.hud.gov/housingcounseling under “Webinar Archives”
- Attendee lines will muted during presentation.
- There may be Q&As. The operator will give you instructions on how to make your comments.

Other Ways to Ask Questions



Your Participation

Please submit your text questions and comments using the Questions Panel. We will answer some of them during the webinar.

You can also send questions and comments to housing.counseling@hud.gov with webinar topic is subject line.

Note: Today's presentation is being recorded and will be provided within 48 hours. The replay information will be sent out via OHC'sISTSERV

Please Mute Your Phones During Discussions

- During the discussions, all the phones may be unmuted by the operator.
- It is critical that you mute your phone during these discussions.
  - Most phones have a Mute function so use it.
  - *6 will also mute and unmute your phone.
- Unmuted phones are a distraction to the discussion.
- Please be courteous.

Brief Survey

- Please complete the brief survey at the end of this session.
- Your responses will help OHC better plan and present our webinars.

Certificate of Training

- If you logged into the webinar, you will receive a “thank you for attending” email from GoToWebinar within 48 hours.
- The email will say that it is your CERTIFICATE OF TRAINING.
- Print out and save that email for your records.

Thank you for attending our XX hour Webinar on XX. We hope you enjoyed our event. This is your CERTIFCATE OF TRAINING. Please print out and save this email for your records.
Please send your questions, comments and feedback to: housing.counseling@hud.gov.

Protecting Personally Identifiable Information

Janice Noble

Acting Chief, Privacy Branch
Office of the Executive Secretariat

Office of Administration

Objectives

- Define Privacy and explain its importance
- Identify key Privacy laws, policies, guidance and principles
- Understand your role in protecting Privacy
- Define Personally Identifiable Information (PII) and list examples
- Protect PII in different contexts and formats
- Recognize potential threats to privacy
- Report a privacy incident

Agenda

- Introduction to Privacy
- Safeguarding Personally Identifiable Information
- Privacy Incidents
- References
- Contact Information

INTRODUCTION TO PRIVACY

What is Privacy?

- **Privacy is a set of fair information practices to ensure:**
  - **Personal information is accurate, relevant and current**
  - **All uses of information are known and appropriate**
  - **Personal information is protected**
- **Privacy also:**
  - **Allows individuals a choice in how their information is used or disclosed,**
  - **Assures that personal data will be used and viewed for business purposes only**
  - **Enables trust between HUD and the American public**

Fair Information Practice Principles

- **The Code of Fair Information Practice Principles established in 1973 at HHS has served as a foundation for future federal privacy frameworks. The eight principles are:**

1. Transparency
2. Individual Participation
3. Purpose Specification
4. Data Minimization
5. Use Limitation
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

Privacy Act

Enacted in 1974 (5 U.S.C. 552a)

- **Develop System of Record Notices (SORNs). A SORN is:**
  - **Any group of records under the control of the Agency where the information is retrieved by a personal identifier.**
    - Post privacy notices on agency Web sites
    - Report annually to OMB

Consequences of Non-Compliance

- **There can possibly be civil and criminal penalties for noncompliance to the Privacy Act. Including:**
  - Employee discipline
  - Fines
  - Criminal charges

Electronic Government (E-Gov) Act Enacted in 2002 (44 U.S.C. S. 101)

- **Requires Agencies to:**
  - Conduct Privacy Impact Assessments (PIAs) for electronic systems
  - Post privacy notices on agency Web sites
  - Designate an Agency Privacy Official
  - Report annually to OMB

Roles and Responsibilities

- **HUD is responsible for following privacy policies and procedures, such as:**
  - Collect, access, use, and disclose personal information only for reasons that are for a legitimate job function and are allowed by law;
  - Safeguard personal information in your possession, whether it be in paper or electronic format;
  - Properly dispose of documents containing PII;
  - Report suspected privacy violations or incidents.

Key Privacy Laws

- **Privacy Act of 1974:** Provides guidance for the collection, use, management, and disclosure of personal information.

- **E-Government Act 2002, title II and III:** Requires federal agencies to assess impact of privacy for systems that collect information about members of the public

Key Privacy Guidance and Policy

- **Office of Management and Budget M-07-16:** Requires safeguards for PII in electronic or paper format and policies and procedures for privacy incident reporting and handling.

- **National Institutes of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J:** NIST provides a structured, standardized set of privacy controls that all systems and organizations must address.

SAFEGUARDING PERSONALLY IDENTIFABLE INFORMATION (PII)

What is PII?

- **Personally Identifiable Information (PII)**
  - Data that can be used to distinguish or trace an individual's identity

- **Sensitive Personally Identifiable Information (SPII).**
  - Social Security numbers, or comparable identification numbers; financial information associated with individuals; and medical information associated with individuals.

Note: Sensitive PII, a subset of PII, requires additional levels of security controls.

Personally Identifiable Information

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
➢Alien Registration Number	➢Sexual orientation
➢Financial account number	➢Account passwords
➢Biometric identifiers	➢Last 4 digits of SSN
	➢Date of birth
	➢Criminal history
	➢Mother's maiden name

Protecting PII Throughout the Information Life Cycle

- **The Information life cycle defines how to handle data from inception to disposition. Protecting PII is important during each stage of the information life cycle.**
  - **Data Collection or Creation. Gathering PII for use**
  - **Data Storage. Maintaining or storing PII**
  - **Data Usage. Using PII to accomplish a job function**
  - **Data Sharing. Disclosing or transferring PII**
  - **Disposition. Disposing of PII when no longer needed in accordance with record management requirements and organizational disposal policies**

Protect PII: LOCK IT UP

- Lock your computer workstation (CTRL + ALT + DELETE)
- Lock your portable devices
- Remove any Card Reader when you are away from the computer
- Lock up documents and files that contain PII

Protect PII: In Transit

- Encrypt PII during transit
- Use an authorized mobile device with encryption to store PII
- Don’t forward work emails with PII to personal email accounts
- Don’t upload PII to unauthorized websites

Protect PII: Beware of Phishing

Phishing is an attempt to steal personal information usually by email. Be suspicious of any email that:

- **You did not expect to receive**
- **Requests you PII (SSN, account number, etc.)**
- **Requires you to urgently take action**
- **Does not look like a legitimate business**

Protect PII: During Travel

- Remember to keep equipment and papers that contain PII in your possession
- Avoid leaving PII in a hotel room unsupervised
- Keep your laptop or other portable devise on your person.

Protect PII: Clean Up

- Don’t leave documents that contain PII on printers and fax machines
- Don’t leave files or documents containing PII unsecured on your desk when you are not there

Protect PII: Faxing

Before faxing:

- Verify recipient's fax number prior to sending PII
- Make sure someone authorized to receive the PII is there to receive the fax
- Use a fax transmittal sheet

- **Receiving faxes:**
  - Quickly retrieve faxes transmitted to you
  - If you are expecting a fax and have not received it, follow-up to ensure the sender has the correct fax number

Protect PII: Mailings

Interoffice:

- Deliver in person when possible
- Send in a confidential envelope
- Follow-up to verify that the recipient received the information

Postal Mail:

- When possible, use a traceable delivery service
- Package in an opaque envelope or container

Protect PII: Telework

- Follow security procedures when removing official records from the office. Get permission from your supervisor to transport, transmit, remotely access or download sensitive information while teleworking.
- Remotely access sensitive information by using authorized methods
- Store sensitive information on HUD authorized mobile devices with appropriate safeguards (encryption)

Protect PII: Disposition

- Review records retention requirements prior to destroying information
- Shred papers containing PII
- Dispose of equipment by returning to OCIO

PRIVACY INCIDENT

Privacy Incident

A Privacy Incident is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar terms referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII whether physical or electronic.

Common Scenarios

- **Privacy Incidents most often occur from:**
  - **Loss, damage, theft, or improper disposal of equipment, media, or papers containing PII**
  - **Accidentally sending a report containing PII to a person not authorized to view the report or sending it in an unprotected manner (unencrypted)**
  - **Allowing an unauthorized person to use your computer or password**
  - **Discussing PII in a public area**
  - **Any security situation that could compromise PII (virus, phishing, etc.)**

How to Report a Privacy Incident

In the event of a potential privacy incident, HUD's third parties and contractors should contact their manager and HUD Liaison. HUD employees are to call HUD's National Help Desk at 1-888-297-8689.

References & Resources

- **The Privacy Act of 1974,**
  http://usdoj.gov/opcl/privstat.htm

- **The E-Government Act of 2002,**
  http://www.whitehouse.gov/omb/memoranda_m03-22/

- **Federal Information Security Management Act of 2002, Title 3 of e-Gov Act of 2002,**
  http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

The Paperwork Reduction Act of 1995,
http://www.gpo.gov/fdsys/pkg/PLAW-104publ13/html/PLAW-104publ13.htm

For additional information on protecting PII, contact the Privacy staff at: Privacy@hud.gov