Protecting PII

Capacity Building Guidance

on Protecting Privacy Information

U.S. Department of Housing and Urban Development

Office of the Chief Information Officer, Office of Privacy

April 2015

Guidance on Protecting Privacy Information

The Department of Housing and Urban Development (HUD) is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with the Privacy Act of 1974, as amended, and other federal privacy-related laws, guidance, and best practices. HUD expects its third party business partners who collect, use, maintain, or disseminate HUD information to protect the privacy of that information.

Definitions

1. Personally Identifiable Information (PII). Defined in OMB M-07-16 as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
2. Sensitive Personally Identifiable Information (SPII). PII that when lost, compromised or disclosed could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers (credit or debit card numbers).

Steps to Take To Help Ensure Compliance

Third party organizations such as Housing Counseling Agencies should take the following steps to help ensure compliance to the Privacy Act and other privacy-related laws:

1. Limit Collection of PII. Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

2. Manage Access to Sensitive PII

    a. Only share or discuss sensitive PII with those who have a need to know for work purposes.
    b. Do not distribute or release sensitive PII to others until the release is authorized.
    c. Before discussing sensitive PII on the telephone, confirm that you are speaking to the right person and inform him/her that the discussion will include sensitive PII. Do not leave messages containing sensitive PII on voicemail.
    d. Avoid discussing sensitive PII if there are unauthorized persons in the adjacent cubicles, rooms, or hallways who may overhear your conversations.
    e. Hold meetings in secure spaces (no unauthorized access or eavesdropping possible) if sensitive PII will be discussed.

f. Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII. Record date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

3. Protect Hard Copy and Electronic Files Containing Sensitive PII

a. Clearly label all files containing sensitive PII. Examples of appropriate labels might include – *For Official Use Only,* or *For [Name of Individual/Office] Use only*.
b. Lock up all hard copy files containing sensitive PII in secured file cabinets. Do not leave sensitive PII in open area unattended.
c. Protect all media (e.g., thumb drives, CDs, etc.) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.
d. Keep accurate records of where PII is stored, used and maintained.
e. Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.
f. Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication and limiting the number of people allowed access to the files.
g. Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

4. Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

a. When faxing sensitive PII, use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, and that all paper waste is disposed of properly (shredded). If possible, use a fax machine that uses a secure transmission line.
b. When sending sensitive PII via email or via an unsecured information system make sure the information and any attachments are encrypted.
c. If a secure line is not available, contact the recipient office prior to faxing to inform them that information is coming. Then, contact the recipient office following transmission to ensure they received it. For each event, the best course of action is to limit access of PII only to those individuals authorized to handle it, create a paper trail, and to verify information reached its destination.
d. Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.
e. Do not let PII documents sit on a printer where unauthorized employees or contractors can have access to the information.

5. Protecting Hard Copy Files Containing Sensitive PII

a. Do not remove records with sensitive PII from facilities where HUD information is authorized to be stored, or access remotely (i.e., from locations other than such physical facilities), unless approval is first obtained from a supervisor.
b. Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention
c. When using the U.S. postal service to deliver information with sensitive PII, double-wrap the document (use two envelopes – one inside the other)and mark only the inside envelope as confidential with the statement – To Be Opened by Addressee Only.
d. If PII needs to be sent by courier, mark "signature required" when sending documents, in order to create a paper trail in the event items are misplaced or lost.

6. Records Management, Retention and Disposition

a. Follow all applicable records management laws, regulations, and policies.
b. Do not maintain records longer than required.
c. Destroy records after retention requirements are met.
d. Dispose of sensitive PII appropriately – permanently erase electronic records. Shred hard copy records.

7. Incident Response. A data breach occurs when PII is viewed, leaked, or accessed by anyone who is not the individual or someone authorized to have access to this information as part of his/her official duties. **Promptly report all suspect compromises of sensitive PII related to HUD programs to HUD's National Help Desk at 1-888-297-8689.**