USAID
FROM THE AMERICAN PEOPLE

Privacy Basics

An Additional Help Reference for ADS Chapter 508

Full Revision Date: 03/07/2014
Responsible Office: M/CIO/IA
File Name: 508saa_030714

This reference has been revised in its entirety.

Privacy Basics

This additional help document answers basic questions about the responsibilities of USAID employees and contract employees to protect the privacy of information about individuals. For this purpose, the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence.

USAID Privacy Program

The Privacy Program supports USAID missions and business functions by assisting the agency in balancing its need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and dissemination of their personal information.

This document will help you to understand the importance of protecting the personally identifiable information (PII) entrusted to USAID, as well as to develop your awareness about how to protect our own PII.

Personally Identifiable Information (PII)

PII refers to 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.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk to the individual and the PII data elements identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

PII is information linked to an individual, including, but not limited to the following:

- Name, former name;
- Social Security Number;
- Date and place of birth;
- Mother's maiden name;
- Personal address, personal telephone number, and personal email address;
- Biometric records (e.g., fingerprints, personal characteristics, iris scans, retina scans, voiceprints, photos);

- Passport number;
- Financial transactions or credit card number; or
- Personal history (e.g., medical, criminal, employment).

PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors, which, *when considered together, can identify an individual*. Because of this *mosaic effect,* consideration needs to be taken when collecting and releasing data elements.

PII is Sensitive But Unclassified (SBU) Information

PII is a type of Sensitive But Unclassified (SBU) information. PII, therefore, requires greater controls against unauthorized access and disclosure than unclassified information. USAID employees must use label documents containing PII with the SBU header and footer and use the green SBU Cover Sheet with paper documents. USAID employees and contract employees must protect PII, as well as other SBU information, against unauthorized access or disclosure by ensuring that only those people who have *a clearly demonstrated need to know or use the information* are given access.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.

Your Responsibilities to Protect PII

All USAID employees and contract employees must understand and carry out their specific responsibilities to protect the PII entrusted to them and to prevent its breach so that USAID retains the trust of the American public.

All USAID employees and contract employees must protect the PII that is entrusted to them. All PII handled, processed, compiled, maintained, stored, transmitted, or reported in our daily work must be protected. To protect PII, USAID employees and contract employees must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what is needed to complete our job duties, and must not disclose PII to unauthorized parties.

USAID must protect PII against anticipated threats or hazards that could result in *substantial harm, embarrassment, inconvenience, or unfairness* to any individual about whom USAID maintains information and to USAID. For more information on your responsibilities to protect PII, see **ADS 545mbd, Rules of Behavior for Users**.

How To Protect PII

A few simple and cost-effective steps may well deliver the greatest benefit against abuse, loss, or theft, such as:

- Use PII only when necessary
- Use only the necessary amount of PII to complete the task
- Share PII only when necessary and only with those who have a "need to know"
- Check for PII in email strings and attachments before sending email outside of USAID approved domains (usaid.gov, state.gov, ofda.gov, oti.gov)
- Only Use USAID email to conduct USAID business
- Use encryption when sending PII by email (e.g., Adobe Acrobat or WinZip)
- If encryption is not available, send the PII in a password protected attachment with the password in a separate email
- Secure PII in locked drawer or cabinet
- Never leave PII on a desk, network printer, fax machine, or copier
- Label documents containing PII with the SBU header and footer and use the green SBU Cover Sheet (AID 630-3 (11/95)) with paper documents to limit unauthorized disclosure
- When viewing PII, use a privacy screen on your monitor
- Lock your computer whenever you leave your station
- Do not permit your computer to remember passwords
- Do not discuss PII within earshot of others without the need to know (for example, in cubicles, hallways, elevators, or restaurants)
- Maintain control over mobile devices (laptops, smartphones, USB flash drives) that contain PII
- Make sure your mobile devices are password protected
- Use a secure fax machine when sending PII by facsimile
- Do not send PII to your home computer or personal email address
- Use the USAID remote access process when working on a computer or mobile device outside of the network
- Do not post PII on shared drives, SharePoint sites, USAID intranet, or public websites
- Do not post PII on Social Media Web sites, unless specifically authorized by the Privacy Office or FOIA Office
- Documents used as examples or for training must not contain actual PII data
- Password protect documents that contain PII
- Follow your program records retention schedule – destroy PII ASAP
- Destroy paper PII by shredding
- Destroy electronic PII according to **ADS 545mas, Media Handling Procedures and Guidelines**

Privacy Breaches

A privacy breach occurs when:

- PII is disclosed to unauthorized parties,
- there is a theft or loss of PII,
- PII is disclosed without the written consent of the individual to whom the record applies (unless required by law),
- there is unauthorized access to PII by unauthorized parties or access by authorized parties without a "need to know" the specific PII involved, or
- there is an unauthorized modification of PII.

Disclosure can be by any means: written, oral, electronic, or mechanical.

You Must Report all Potential or Actual Privacy Breaches

All USAID employees and contract employees must report immediately upon discovery *all potential and actual* privacy breaches to both the CIO Helpdesk at 202-712-1234 or **CIO-HELPDESK@usaid.gov** ***and*** the Privacy Office at **privacy@usaid.gov**, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred.

For additional information about what is PII, how to protect PII, privacy breaches, and your responsibilities, please contact the Privacy Office at privacy@usaid.gov.

If you do not have it, you cannot lose it!