Privacy 101

Awareness and Best Practices

Revised (May 10, 2021)

GPO Protection of Personally Identifiable Information (PII)

- **What is Privacy**

Broadly, PII is "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." (Ref.: OMB Memorandum 07-16.)

It is more than "information security" **Information security is primarily about protecting data in order to preserve its "confidentiality, integrity, and availability** (National Institute of Standards & Technology, Commerce Dept. — NIST)

It is more than "information security" Because personal data can be used to determine individuals' rights, benefits, privileges, freedoms, reputation **"Privacy" recognizes that individuals must have a role in the collection, maintenance, use, and disposition of their personal data.**

Federal Data Privacy Framework

- **Privacy Act of 1974, 5 U.S.C. 552a**

  Implemented Fair Information Practice Principles (FIPPS) Responded to public concerns about covert… Government information collection activities

- **E-Government Act of 2002 (EGOV)**

  Move Federal services and programs online Encourage citizen access and participation Increase transparency

- **Other Federal laws, policies, frameworks, and guidance**

  NIST Publication 800-122 (2010)

  Protection of Sensitive Information — OMB 06-16 (2006)

  Data Breaches — OMB 17-12 (2017)

  Tracking/Customization Technologies — OMB 10-22 (2010)

  Access to Agency's Privacy Program OMB 17-06 (2016)

  Identity Monitoring for Agency employees — OMB 16-14 (2016)

GPO Protection of Personally Identifiable Information (PII)

- **GPO Directive 825.41B**
- **Purpose**

  To establish a framework for the protection of personally identifiable information (PII) at the U.S. Government Publishing Office. **The loss, compromise, or disclosure of PII may lead to identity theft or other fraudulent use that could result in substantial harm, embarrassment, inconvenience, or unfairness to individuals.** Appropriate measures are therefore necessary to protect PII and Protected Health Information (PHI) (collectively termed PII) from unauthorized use, access, disclosure, or sharing and to protect relatedinformation systems from unauthorized access, modification, disruption, or destruction.

Handling Rules for PII

Paper Form

- **Storing PII:** Lock cabinets when not in use.
- **Transporting PII:** Physically between approved locations and with prior authorizations.
- **Destroying PII:** Cross cut shredding.

Electronic Form

- **Transmitting PII:** Between facilities or through e-mail
- Encrypt at rest
- Encrypt when transmitted
- Authorized users only

In accordance with GPO Directive 825.41B.

Handling Rules for PII (Continue)

Special handling required to protect privacy data or sensitive data includes:

- **Labeling**: Personally Identifiable Information (PII) as “For Official Use Only” (FOUO) Destroying PII:
- **Accessing:** Only what is necessary to complete a work-related duty or job
- **Disclosing:** Verbal, paper, and electronic PII only within and between authorized entities to conduct official business

In accordance with **GPO Directive 825.41B**.

What are PII Data Breaches?

Privacy Data Breaches are Inappropriate Disclosures of Personally Identifiable Information (PII), Protected Health Information (PHI), or Business Sensitive Information (SI) that may:

- Be lost, stolen, compromised
- Be unauthorized disclosure, acquisition, or access
- Be intentional or accidental
- Affect high-risk or low-risk
- Be found immediately or after a delay

Also referred to as a PII Incident

PII Incident Reporting

Privacy (PII) Incident Report pertaining to GPO employees and GPO contracts

Provide Details

- When reporting a Privacy (PII) incident, submit GPO Privacy Incident Reporting Form (Form 4049, available to GPO employees on GPO Intranet), and provide as much detailed informationas possible about what occurred, when did the incident occur and what information was compromised.
- Any paper documentation, webpage URL or system process information from the breached should be reported to GPO.
- GPO will take appropriate action to mitigate the effects of the incident and report its findings as determined by the GPO Privacy Office.

PII Incident Reporting (Continue)

Public reporting of PII on GPO websites

- GPO's govinfo website hosts the USCOURTS collection on behalf of the Administrative Office of the U.S. Courts (AOUSC).
- Individuals while searching the net may discover their personal information is associated with a court opinion published in the govinfo website. This can result in the individual submitting an inquiry asking for the opinion to be removed.
- Public can email directly to the Administrative Office of the U.S. Courts at Court_Opinions@ao.uscourts.gov."
- **Please note:** All such public PII inquiries are passed to AOUSC. Only AOUSC can interpret the opinion's appropriateness for public accessibility and only the AOUSC can direct GPO to remove content from this collection

Basic Privacy Best Practices

- Understanding the importance of PII protection.
  If you collect it, you must protect it!

- Identifying best practices for protecting & retaining PII.
  Think PRIVACY when handling PII!

- **Don't keep it longer than needed!**
  Can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identify theft or other fraudulent use of information.

GPO Privacy Program Point of Contact

MANJIT S. TANEJA
GPO Privacy Officer
Office of Chief Information Officer (OCIO)

U. S. Government Publishing Office
732 North Capitol Street, N.W.
Washington, DC 20401
202.512.1652
privacy@gpo.gov