GPO

ANNUAL PRIVACY BRIEFING

PRIVACY AWARENESS AND BEST PRACTICES PII - 101

(Mandatory training for all GPO Employees and Contractors)

Prepared by:
GPO Privacy Office
Information Technology

Fiscal Year 2023

What is a Privacy?

Privacy – ***is the right of individuals to determine for themselves when, how, and to what extent information about them is collected and communicated to others.*** Concern being, their private information in wrong hands can potentially inflict harm to them, and compromise their personal or professional status.

Individuals in this context could be an employee, a contractor, a customer, a vendor, or public.

Privacy is an asset, and has become a core value of democratic societies.

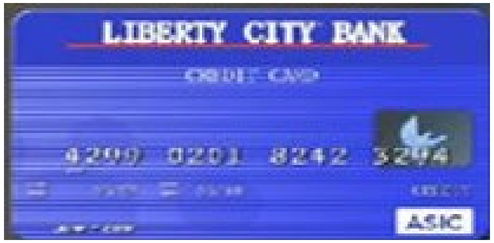
Today, it is being treated as an essential aspect of freedom and human dignity.

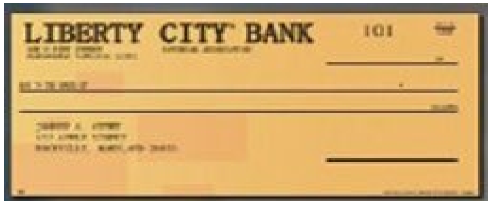
Privacy – No doubt, it is deeply associated with Information Systems Security – However, please note - Privacy is much more than just "Information Security".

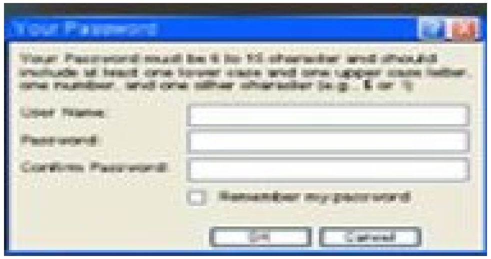
Privacy requires an organization to consider:

- Safeguarding interests of individuals and extending them rights in their data collection, maintenance, use, and disposition. Yes, individuals have right to ask for corrections.
- Informing them regarding collection of their personal information (including health information), giving them choice (where applicable), making them aware of the purpose why their PII, is being collected, due process, and mitigation options in case of a breach.
- As the Internet and social media explode, the privacy domain is expanding too. Factually, it now expands to employees' Internet activity, visits to medical unit, telephone conversations, emails, and workspace privacy. Refer to GPO Directive 825.33C

What is PII?







Your Password must be 6 to 15 character and should include at least one lower case and one upper case letter, one number, and one other character (e.g., $ or !)

User Name

Password

Confirm Password

□ Remember my password

"Personally Identifiable Information (PII) is "information which can be used to distinguish or trace an individual's identity… when used alone, or when combined with other personal or identifying information".

GPO Directive 825.41B defines PII as "...information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), 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."

GPO Directive 825.41B
OMB Memorandum 07-16.

What are examples of PII?
Here is a partial list:

- ✓ Social Security Number, full or truncated
- ✓ Birth date, place of birth – Citizenship and legal status
- ✓ Educational or employment records
- ✓ financial transactions, direct deposit information, credit card or bank account numbers
- ✓ medical information
- ✓ criminal history that contains name, payroll number, social security number
- ✓ name combined with date of birth or place of birth
- ✓ other identifying particulars, such as a finger or voice print or a photograph
- ✓ Spouse information, marital status, and child information

Sensitive & Non-Sensitive PII

By the definition of **Department of Homeland Security** 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."

Non-Sensitive PII can be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.

Sensitive PII (hard copy, or digital) include, but not limited to* :

- SSN, full and truncated,
- Birth date/place, citizenship and legal status,
- Name (other names used), mother's maiden name,
- Driving License, Passport, Alien Number,
- Financial information: credit cards, deposits, etc.,
- Medical, biometric or disability information,
- User IDs/Passwords,
- Emergency contact information,
- Gender, race/ethnicity - religious preference,
- Spouse, marital status, and child information,
- Criminal or employment history,
- Security clearance, military records.

** OMB Memorandum M-07-16*

Non-Sensitive PII

PII is always sensitive, but considering the possible impact some PII can be categorized as non-Sensitive PII which include, but are not limited to:

- Personal email address,
- User IDs,
- Mailing and home address,
- Home and personal cell telephone numbers,
- Emergency contact information,
- Resumes that do not include an SSN or where the SSN is redacted,
- General background information about individuals found in resumes and biographies
- Position descriptions and performance plans without ratings.

Protected Health Information – PHI

PHI – call it Protected Health Information, Personally Identifiable Health Information, or just Personally Identifiable Information (PII) that contains an individuals' private health information.

PHI generally shows up in the following:

- Medical Folder (Physical or electronic).
- Correspondence from doctor (emails/printed/written).
- Lab results (Blood test reports/Radiology films & reports/Physicians' notes)
- Phone records/Emails/Fax.
- Medical Unit Visit records (Verbal/written /Computer System).
- Computer/Tablet/Phone/Electronic Storage.

PII/PHI (paper or electronic) include, but not limited to*:

- SSN (full and truncated).
- Birth date, place of birth – citizenship and legal status.
- Name (other names used) mother's maiden names.
- Medical, biometric or disability information.
- Health Plan (Insurance) account numbers.
- Driver license, passport – alien numbers.
- Financial /Credit Accounts.
- Passport type photograph.
- User IDs and passwords .
- Emergency contact information.
- Gender, race/ethnicity - Religious preference.
- Spouse information, marital status, and child information.
- Criminal or employment history.
- Security clearance.
- Military records .

* *OMB Memorandum M-07-16*

Protected Health Information – PHI … Continue

The Health Insurance Portability and Accountability Act identifies (HIPAA)

It promulgates standards and/or rules to promote and monitor PII/ PHI compliance.

Please note:
GPO takes PHI very seriously and GPO embraces spirit of HIPPA however, HIPPA as a law does not apply to GPO.

Do we know our PII is at risk all the time...

IdentityForce, a leading provider of proactive identity, privacy and credit protection, publishes PII incidents each year.

Here is a partial list.

Source - IdentityForce.

January, 2021:

- **Socialarks.** A Chinese social media management company lost PII of at least 214 million Facebook, Instagram, and LinkedIn users. Information included names, phone numbers, email addresses, profile pictures, etc.

February, 2021:

- **California DMV.** Attackers grabbed drivers' PII from the last 20 months of vehicle registration records, including names, addresses, license plate numbers, and vehicle identification numbers (VINs).
- **T-Mobile.** Undisclosed number of customers' bank accounts, names, addresses, email addresses, account numbers, SSNs, account security questions and answers, date of birth, etc., were compromised.

April, 2021:

- **Facebook.** The personal data of 533 million Facebook users, including phone numbers, full names, locations, email addresses and biographical information, from 106 countries was posted online for free in a low-level hacking forum.
- **LinkedIn.** Over 500 million user profiles were discovered on the Dark Web. The hackers shared two million of these records, including their names, LinkedIn account IDs, email addresses, phone numbers, gender, et., for a fee of $2 each.

June 2021:

- **Volkswagen & Audi.** The personal information of 3.3 million customers of Volkswagen and Audi was exposed. Data included names, mailing addresses, emails, and phone numbers.

Our PII is at risk as we speak... (Continue)

Country	Fullz price on dark web (average, US$)
USA	$8
UK	$14
Turkey	$14
Israel	$14
China	$15
Singapore	$15
Canada	$15
Australia	$15
New Zealand	$20
UAE	$25
Japan	$25
Europe	$25

Price of "Fullz", which is the full credentials e.g. SSN, name, DOB etc. Source: Comparitech.

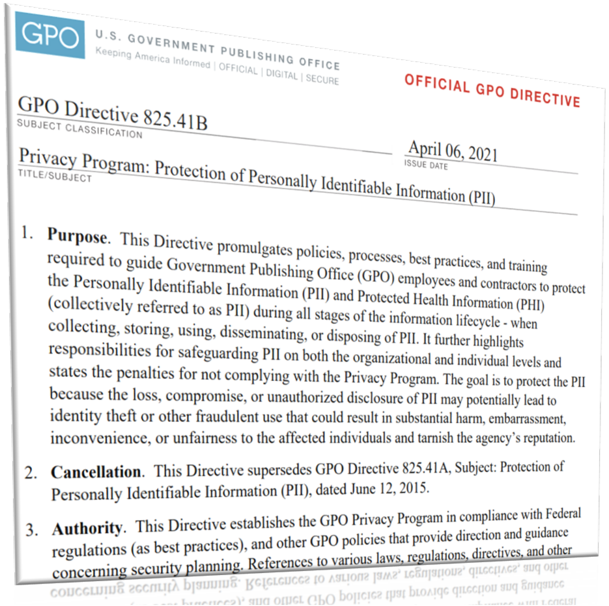
- SSNs stolen at Defense Information Systems Agency (February 2020)
- A Microsoft Power Apps - breach exposed 38 million records containing PII and impacted 47 organizations, including public health agencies (August 2021).*
- OPM was hacked - 21.5 million individuals were impacted.
- Veterans Administration – 26 Million PII records impacted.
- IRS - 47 million IRS Transcripts were accessed.
- FEMA - About 2.5 million disaster victims.
- In 2019, Facebook, Instagram, Microsoft, and WhatsApp were hit.
- Android Users Data Leak - 100+ million.
- Facebook — 553 million.
- LinkedIn — 700 million.
- Cyber Security Firm Cognyte — 5 billion.

Cybercriminals sell personal information of the US citizens on a dark web. Full credentials of one person - SSN, name, DOB, etc. was priced $8 in 2021**.

Comparitech reports about 40+ dark web marketplaces that sells stolen identities, credit cards and hacked PayPal accounts.***

* UpGuard Cybersecurity Company
** Security Magazine | The top data breaches of 2021
*** Comparitech

GPO Privacy Program



GPO U.S. GOVERNMENT PUBLISHING OFFICE
Keeping America Informed | OFFICIAL | DIGITAL | SECURE

OFFICIAL GPO DIRECTIVE

GPO Directive 825.41B
SUBJECT CLASSIFICATION

April 06, 2021
ISSUE DATE

Privacy Program: Protection of Personally Identifiable Information (PII)
TITLE/SUBJECT

1. **Purpose**. This Directive promulgates policies, processes, best practices, and training required to guide Government Publishing Office (GPO) employees and contractors to protect the Personally Identifiable Information (PII) and Protected Health Information (PHI) (collectively referred to as PII) during all stages of the information lifecycle - when collecting, storing, using, disseminating, or disposing of PII. It further highlights responsibilities for safeguarding PII on both the organizational and individual levels and states the penalties for not complying with the Privacy Program. The goal is to protect the PII because the loss, compromise, or unauthorized disclosure of PII may potentially lead to identity theft or other fraudulent use that could result in substantial harm, embarrassment, inconvenience, or unfairness to the affected individuals and tarnish the agency's reputation.

2. **Cancellation**. This Directive supersedes GPO Directive 825.41A, Subject: Protection of Personally Identifiable Information (PII), dated June 12, 2015.

3. **Authority**. This Directive establishes the GPO Privacy Program in compliance with Federal regulations (as best practices), and other GPO policies that provide direction and guidance concerning security planning. References to various laws, regulations, directives, and other

GPO 825.41B directive states appropriate measures to protect PII from unauthorized use, access, disclosure, or sharing and to protect related information systems from unauthorized access, modification disruption, or destruction.

Handling PII - GPO rules

GPO Directive 825.41B requires handling PII as following:

PII in paper

✓ **Storing:** Lock cabinets when not in use.

✓ **Transporting:** Physically between approved locations and with prior authorizations.

✓ **Transmit** either in person or through FedEx or U.S. Postal Service with tracking and delivery notification.

✓ **Destroying:** Cross cut shredding.

Both paper and digital form PII

✓ **Labeling**: "For Official Use Only" (FOUO) .

✓ **Identifying** properly the data as "Sensitive PII".

✓ **Disclosing**: Verbal, paper, and electronic PII only within and between authorized entities to conduct official business.

PII in digital form

✓ **Encrypt** at rest and when transmit using GPO authorized encryption algorithms (see IT Security Policy Directive, 825.33C).

✓ **Available** authorized users only.

✓ **Notify** the receiver(s) that they are expected to continue to protect the data using encryption or comparable controls and to immediately report any actual or suspected loss of integrity.

✓ **Remote access.** Users must have a business need to remotely access PII on a GPO network or system. Such access to the GPO network is permitted only in conformity with GPO IT Directive 825.35B. Exceptions are permitted when authorized by the Director, or his or her designee.

✓ **Downloading** PII on external storage is prohibited unless such devices are provided by the agency.

What are PII / PHI Data Breaches?

Privacy data breaches are inappropriate disclosures of PII that may:

- Be lost, stolen, or compromised PII
- Be intentional or accidental
- Affect high-risk or low-risk PII
- Be found immediately or after a delay

Privacy Incidents

Are events in which there is knowledge or reasonable belief that there has been unauthorized or inappropriate use, access, disclosure, loss, transfer, modification, and and/or exposure of PII. It could be intentional or accidental. It could affect high-risk or low-risk PII. It may be found immediately or after a delay.

Privacy Breach

Is a confirmed unauthorized or inappropriate collection, use, access, disclosure, transfer, modification, and/or exposure of PII. An encrypted PII is not considered to be accessible to an unauthorized person; thus, a compromise of encrypted information is not a Privacy Incident.

Some potential Breach Scenarios

- HR/Payroll/Medical/Education.
- GPO website has un-redacted PII.
- PII on our servers (GPO/Cloud/Hosted)
- PII in emails being sent/received
- PII on other than electronic media being shipped/received
- Breach of GPO customer provided PII at GPO facility, Contractor facility, during shipment, electronic transfer, at Contractor facility, etc.
- Public issue with PII on a GPO website document.

Human error is the cause of 80 percent of the PII breaches. Not knowing or not following guidance, or just being careless can result in the unintended disclosure of privacy sensitive information and potentially adversely affect many personnel.

SSN is the **most** frequently lost, stolen or compromised PII data element.

SSN is involved in almost 70 percent of breaches. **This sensitive identifier must be closely safeguarded or eliminated from use.**

SSNs are improperly disclosed by sending SSNs in an email or in attachments, creating recall rosters with SSNs, or posting names with associated SSNs to web portals or shared drives. In these examples, SSNs were either transmitted without encryption, not properly marked or sent to recipients that did not have a need to know.

Reporting PII Data Breaches

How do GPO employees and GPO contractors report PII? (Based on the internal Privacy Incident Reporting procedures?

#1 Always, immediately notify your supervisor. Access the GPO **4049 Privacy Incident Reporting Form** available at the GPO Intranet website.

#2 Contact your Business Unit manager or Business Unit PII Point of Contact. Provide a copy of the completed incident reporting **Form 4049.**

Privacy (PII) Incident Report: Provide Details

When reporting a Privacy (PII) incident, provide as much detailed information as possible about what occurred, when did the incident occur and what information was compromised.

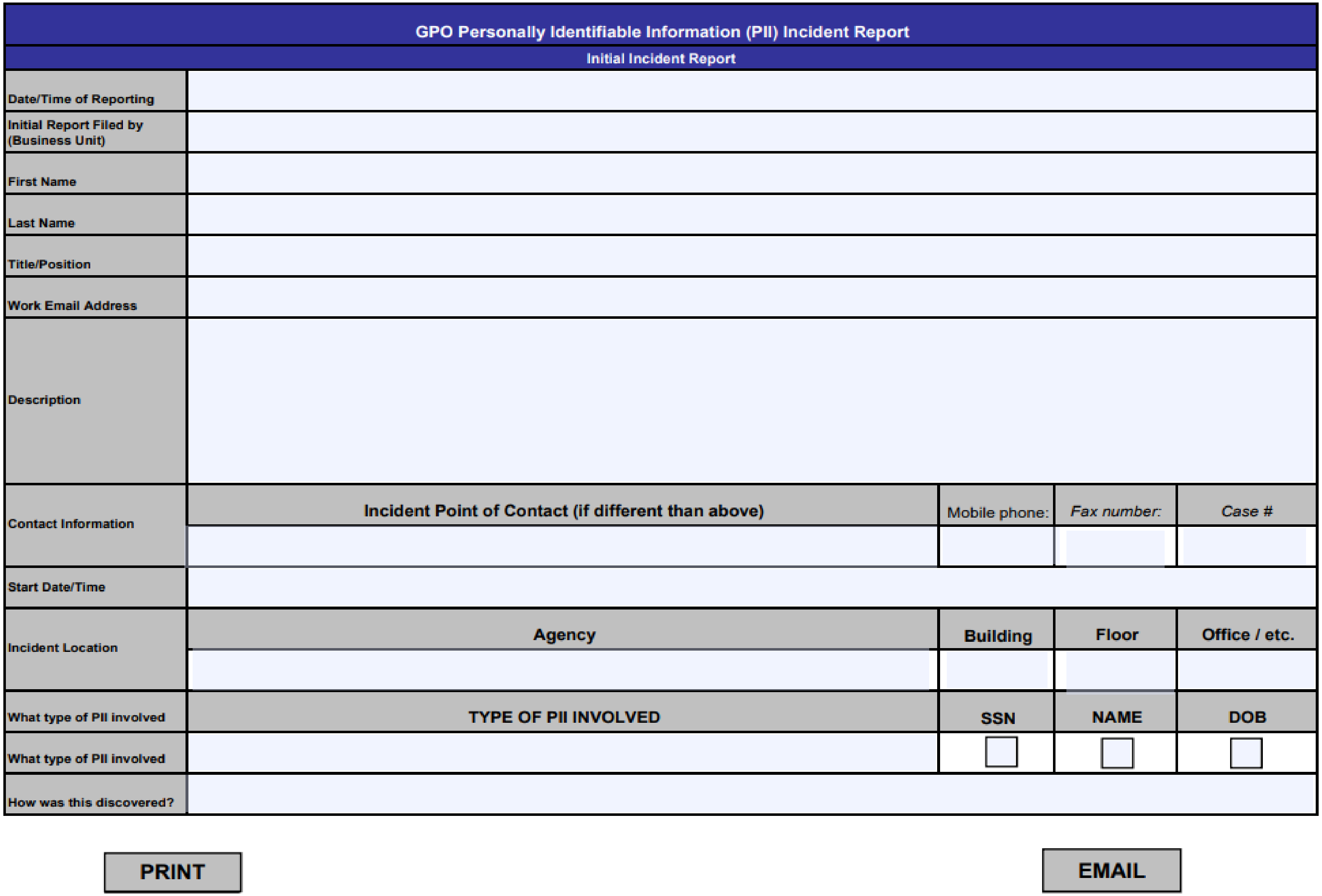
Any paper documentation, webpage URL or system process information from the breached should be reported to GPO.

GPO Privacy Incident Response Team (PIRT) will take appropriate action to mitigate the effects of the incident and report its findings as determined by the GPO Privacy Office.

Form 4049 requires to include as much information as possible to PII Incident Report. This include:

- Date/Time of Reporting
- Initial Report Filed by
- (Business Unit)
- First Name
- Last Name
- Title/Position
- Work Email Address
- Description
- Contact Information
- Incident Point of Contact (if different than above)
- Mobile phone: Fax number: Case #
- Start Date/Time
- Incident Location
- Agency Building Floor Office / etc.
- What type of PII involved
- How was this discovered?

Reporting PII Data Breaches (4049 form)



GPO Personally Identifiable Information (PII) Incident Report

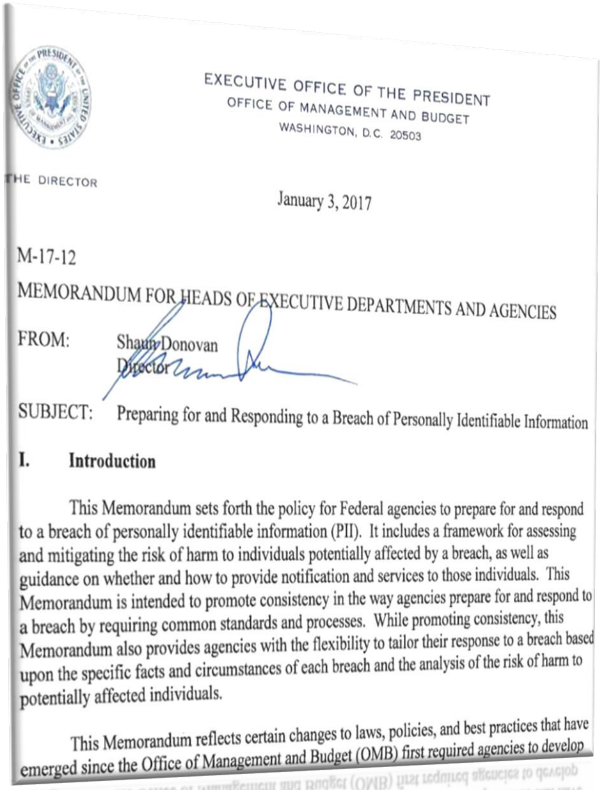
Initial Incident Report

Date/Time of Reporting				
Initial Report Filed by (Business Unit)				
First Name				
Last Name				
Title/Position				
Work Email Address				
Description				
Contact Information	Incident Point of Contact (if different than above)	Mobile phone:	*Fax number:*	*Case #*
Start Date/Time				
Incident Location	Agency	Building	Floor	Office / etc.
What type of PII involved	TYPE OF PII INVOLVED	SSN	NAME	DOB
What type of PII involved		□	□	□
How was this discovered?				

PRINT

EMAIL

PII incidents possible scenarios



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

January 3, 2017

M-17-12

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Preparing for and Responding to a Breach of Personally Identifiable Information

I. Introduction

This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII). It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This Memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes. While promoting consistency, this Memorandum also provides agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

This Memorandum reflects certain changes to laws, policies, and best practices that have emerged since the Office of Management and Budget (OMB) first required agencies to develop

According to OMB, “common” examples of a PII breaches are following:

- a laptop or portable storage device storing PII is lost or stolen;
- an email containing PII is inadvertently sent to the wrong person;
- a box of documents with PII is lost or stolen during shipping;
- an unauthorized third party overhears agency employees discussing PII about an individual seeking employment or federal benefits;
- a user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;
- an IT system that maintains PII is accessed by a malicious actor; or PII that should not be widely disseminated is posted inadvertently on a public website.

Hypothetically, GPO employees and contractors also might experience with such undesired situations.

What to do?

1. **Immediately notify your supervisor.**
2. **Take the GPO 4049 Privacy Incident Reporting Form available at the GPO intranet and write down all the details.**
3. **Email and provide copy of the form to your BU manager or PII Point of Contact at your BU.**

GPO

Basic Privacy Handling – Best Practices

GPO 825.41B directive requires to:

- To provide the Privacy Directive via Intranet and GPO web site,
- Publish PII collection, storage, and handling guidelines (for internal use),
- Provide required privacy training to employees and contractors.
- Make employees and contractors aware of best practices, penalties and implications of not following the guidelines published in GPO Privacy Directive 825.41B.

Best Practices

If you collect PII, you must protect it. Think PRIVACY when handling PII.

- ✓ Protect sensitive PII (Hard copy or electronic)
- ✓ Use it in a controlled access area.
- ✓ Do not leave PII unattended on display screen, desks, printers.
- ✓ Keep it in a locked and secured area, when not in use.
- ✓ Don’t keep it longer than needed.

- ✓ If you happen to see unprotected PII document or display, inform your supervisor i mmediately.

When a system containing PII is disposed of, the PII must be securely expunged with a log maintained of expunging activity. Further, if the hardware equipment holding any PII is either being retired, disposed of, changing ownership, or sent for repairs, it must be ensured the PII held on the equipment becomes permanently non retrievable by any means.

PII In Email:

- ✓ Encrypt all PII information before transmitting either internally or externally
- ✓ CALL the recipient in person to give them the password
- ✓ Do not convey passwords through voicemail
- ✓ DO NOT SEND the password in an email.

PII In Fax:

- ✓ Ensure the recipient will be present to pick up the fax immediately.
- ✓ Contact the recipient directly to confirm receipt.
- ✓ Always use a cover sheet

PII In Regular Mail:

- ✓ Must be sufficiently sealed to prevent accidental opening
- ✓ Must be sealed in a manner so that signs of tampering will be easily available

Best Practices

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 it off site, use a GPO-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, GPO-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 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.

Posting Sensitive PII to websites and shared drives: Do not post Sensitive PII on the GPO 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."

GPO Directive 825.41B

Risks for not Safeguarding PII

Following deliberate, or accidental actions are prohibited by the GPO Directive 825.41B

- ✓ Removing, concealing, altering, damaging, destroying deleting, loosing, unapproved sharing, or using PII for personal purposes.

The following penalties could potentially apply to an individual who fails to comply with regulations for safeguarding PHI

As per GPO Privacy Directive 825.41B, employees who fail to protect PII according to established standards and procedures or who disclose PII improperly may be subject to disciplinary action up to and including removal or criminal sanctions and penalties in appropriate cases.

.

Contractors who fail to protect PII may be subject to termination for default and any other appropriate administrative action.

New employees should fill a “Rules of Behavior Form” (IT Security Form) to acknowledge their awareness of and understanding the importance of safeguarding information, risks associated with any breach, and penalties for not following the specified guidelines.

Any Questions –
Contact GPO Privacy Program

GPO Privacy Office
Information Technology

U. S. Government Publishing Office
732 North Capitol Street, N.W.
Washington, DC 20401
(202) 512-1652

mtanjea@gpo.gov
privacy@gpo.gov