GPO BASIC PRIVACY AWARENESS AND BEST PRACTICES

This training is designed to enhance privacy awareness at the GPO.

It provides foundational information on privacy, including best practices for privacy compliance and safeguarding, the risks associated with data breaches, and the responsibilities involved in maintaining privacy protection standards.

GPO

GPO Privacy Office | Information Technology

BOOKSTORE
An investment in knowledge pays the best interest.
BENJAMIN FRANKLIN
GPO
U.S. GOVERNMENT PUBLISHING OFFICE
710
BOOKSTORE
KEEPING AMERICA INFORMED
GPO

The Privacy Office of the Government Publishing Office is excited to welcome you to this vital training. This training reflects our ongoing commitment to safeguarding personal information and upholding the highest privacy standards.

As outlined in GPO Privacy Directive 825.41C (Privacy Program: Protection of Personally Identifiable Information, PII) and Directive 825.33D (GPO IT Security Program Statement of Policy), all employees are required to protect PII. This responsibility is essential to maintaining public trust and ensuring the integrity of our operations.

This training aims to equip GPO employees and contractors with the knowledge to understand and comply with all privacy-related requirements, fostering the environment for protecting privacy at GPO.

We appreciate your dedication to protecting privacy at GPO.

Sincerely,
GPO Privacy Office,
Information Technology

Table of Contents

Training Information

Audience: All GPO employees and contractors.

Before accessing the GPO computer systems, new employees and contractors must complete this training (available on the GPO public website) as part of the onboarding process.

Expected time to complete: Approximately 1.5 hours.

Acknowledgment Statement: Please complete the Acknowledgement Statement form provided at the end of this document and submit it to your onboarding officer and the Privacy Office at privacy@gpo.gov.

Photos: All the visuals belong to GPO and Microsoft Word Stock images.

For questions, Contact the GPO Privacy Office at privacy@gpo.gov

Links to the referenced sources & documents are published at the end of this document.

Definitions

What is Privacy?

Privacy – is the right of individuals to determine for themselves - when, how, and to what extent information about them is collected and shared with others. These individuals may include employees, contractors, customers, vendors, or members of the public.

Privacy is a core value of democratic societies and is essential to freedom and human dignity.

In general, privacy requires organizations to:

- Safeguard the interests of individuals by granting them rights regarding the collection, maintenance, use, and disposition of their data.
- Inform employees about the collection of their PII, including why it is being collected, the process involved, and available mitigation options in case of a breach. For example, individuals requesting secure credentials are informed when completing their applications.
- Provide individuals with choices (where applicable), such as the right to request corrections to their information.
- Extend privacy considerations to employees' Internet activity, visits to medical units, telephone conversations, use of conferencing/communication tools (e.g., MS Teams, Zoom, Webex), emails, and workspace as the scope of privacy evolves in the digital age.

What is PII?

Per Memorandum 17-12 of the Office of Management and Budget (OMB):

According to the Office of Management and Budget (OMB) Memorandum 17-12:

> "PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

Per GPO Directive 825.41C:

> "PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

Who are Employees and Contractors?

Employees and contractors are teammates with access to the GPO network and use GPO-provided computers.

What is PHI?

The Health Insurance Portability and Accountability Act (HIPAA) defines Protected Health Information (PHI) as an individual's health, treatment, and payment information, as well as any additional information maintained within the same designated record set that could identify the individual or when combined with other information, be used to identify the individual.

In this training, PII & PHI are collectively referred to as PII.

GPO employees and contractors (regardless of their work area) may encounter PHI in the following sources:

- Medical folders containing health, biometric, disability, health insurance, and emergency contact information.
- Correspondence from the doctor.
- Lab results and physicians' notes.
- Phone records/emails/fax.
- Medical unit visit records (in any form).
- Employment, security, and medical insurance documents.

HIPAA establishes standards and/or rules to promote and monitor compliance with PII/PHI protection.

Note: *HIPAA is an executive branch regulation that does not apply to GPO. However, the GPO Privacy Office (PO) recommends adopting HIPAA regulations as a best practice.*

What is a privacy incident?

A privacy incident is an occurrence (event) that has the potential to compromise the privacy or confidentiality of personal information. It may result from accidental or deliberate unauthorized access, use, disclosure, alteration, or destruction of personal data.

What is a privacy breach?

A privacy breach is an incident that results in the confirmed disclosure of personal data, not just potential exposure, to an unauthorized individual.

What is a PII disclosure?

Disclosure means to permit access to or the release, transfer, or other communication of PII by any means. Disclosure can be *authorized*, such as when a GPO Office of Finance can see and process financial records of employees and contractors.

Disclosure can also be *unauthorized* or inadvertent (accidental). An unauthorized disclosure can happen due to a data breach or a loss, and an unintentional disclosure can occur when data released in public reports are unintentionally presented in a manner that allows individual persons to be identified (as defined by the U.S. Department of Education).

List of PII Data *(From OMB 17-12)*

OMB Memorandum 17-12 *(Appendix I: Model Breach Reporting Template)* recommends reporting unauthorized disclosure of these PII data elements in case of a privacy incident. In other words, this document considers the following list of PII elements to be the data elements that can be used to distinguish or trace an individual's identity, alone or when combined with other information linked or linkable to a specific individual.

Identifying Numbers

- Social Security Number (SSN)
- Patient ID number
- Student ID number
- Passport number
- DOD ID number
- Employee identification number
- Taxpayer identification number
- Credit/Debit card number
- Vehicle identification number
- Personal bank account number
- Personal mobile phone number
- License plate number
- Federal student aid number
- Alien registration number
- DOD benefits number
- Truncated or partial SSN
- Driver's license number
- File/Case ID number
- Personal device identifiers or serial numbers
- Business credit card number (sole proprietor)
- Business bank account number (sole proprietor)
- Business mobile number (sole proprietor)
- Business taxpayer identification number (sole proprietor)
- Business vehicle identification number (sole proprietor)
- Business device identifiers or serial numbers (sole proprietor)
- Health plan beneficiary number
- Professional license number

Biometric/Emergency Information

- Fingerprints
- Retina/Iris Scans
- Hair Color
- Video recording
- DNA Sample or Profile
- Palm prints
- Eye color
- Dental profile
- Photos
- Signatures
- Vascular scans
- Scars, marks, tattoos
- Height
- Voice/ Audio recording
- Weight

List of PII Data *(From OMB 17-12) (Continued)*

Biographic information

- Name (including nicknames)
- Date of birth (day, month, year)
- Country of birth
- Citizenship
- Home address
- Group/Organization membership
- Business mailing address (sole proprietor)
- Personal e-mail address
- Personal financial information (including loan information)
- Education information
- Gender
- Ethnicity
- City or county of birth
- Immigration status
- Zip code
- Sexual orientation
- Spouse information
- Military service information
- Business phone or fax number (sole proprietor)
- Business e-mail address
- Business financial information (including loan information)
- Race
- Nationality
- Marital status Religion/Religious preference
- Home phone or fax number
- Children information
- Mother's maiden name
- Global positioning system (GPS)/location data
- Employment information
- Alias (e.g., username or screenname)
- Professional/personal references
- Resume or curriculum vitae

Medical/Emergency Information

- Medical/Health information
- Workers' compensation
- Mental health information
- Patient ID Number
- Disability information
- Emergency contact

Device Information

- Device settings or preferences (e.g., security level, sharing options, ringtones)
- Cell tower records (e.g., logs, user location, time, etc.)
- Network communications data

Specific Information / File Types

- Taxpayer information/Tax return information
- Civil/Criminal history
- Case files
- Law enforcement information
- Academic and professional background
- Credit history
- Security clearance
- Background check information
- Health information
- Personnel files

PII Categories: Direct and Indirect Identifiers

Reviewing the list provided in OMB Memorandum 17-12, we can see that almost every data element, even *device ringtones*, can be considered PII.

Some PII elements, such as SSNs, can directly identify individuals without additional information. These types of data elements are referred to as *Direct Identifiers.*

Other data elements, however, are insufficient to identify individuals on their own. For example, a standalone date of birth, such as “January 1, 2025,” is insufficient to identify a person without additional context. However, when combined with other data elements, such as “Date of birth: January 1, 2025. Citizenship: USA,” a simple calendar date can become a PII element—although still insufficient to uniquely identify an individual. These types of data elements are called Indirect Identifiers or Quasi-Identifiers. When additional information, such as a ZIP code or street name, is added, the combination may be sufficient to identify an individual within a larger population uniquely. Each piece of information acts like a puzzle piece that reveals the whole picture when combined with others.

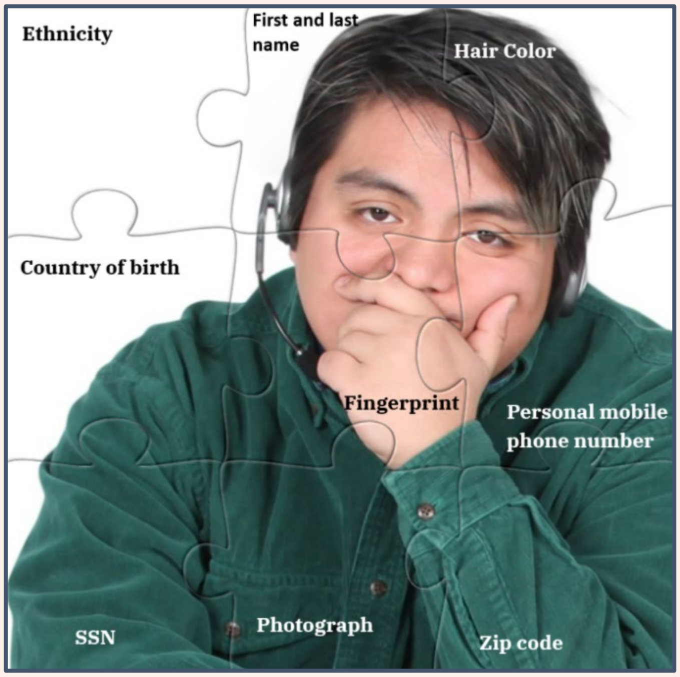


Figure 1. Generic image.

Case Study 1: Identifiers.

Imagine we have only a single piece of the puzzle from an image (Figure 1) - the hair color is black. This information alone is insufficient to identify a specific individual. If we add a ZIP code to the information, it still cannot help much, as hundreds of individuals with black hair could live in the same ZIP code. However, if we include first and last names, this combination significantly narrows the search and may help identify the individual.

Conclusion: A combination of several indirect identifiers can be used to identify individuals.

Which of these data elements (on the puzzle) can be considered a direct identifier? In other words, which PII elements would be enough to recognize an individual even without other puzzle elements?

Go to the Case Study Explanations page *(CTRL+ left mouse clicks)* to see our version of the list of direct identifiers.

PII Categories: Sensitive and Non-Sensitive PII

Identifying individuals is not the only consequence of unauthorized PII disclosure. Identified individuals can be subject to at least targeted marketing campaigns, but in many cases, their personal information can be used to harm impacted individuals financially, morally, and even physically.

Consider the following scenarios:

1. **Name, date and place of birth, email address have been compromised.**
   A combination of these elements can be enough to identify an individual. It is unsettling to know that a combination of these data elements is in nefarious hands. Potential risks include being disturbed, receiving undesired emails, or falling victim to social engineering attacks to obtain even more sensitive PII.

2. **SSN, Bank Account Number, or Medical Diagnosis compromised.**
   When highly sensitive information like an SSN, bank account number, or medical diagnosis is exposed, the potential harm is severe and can have long-lasting effects. These include identity theft, financial loss, discrimination, stress, anxiety, and frustration.

Based on the potential risk of harm, PII data elements are categorized as sensitive and non-sensitive:

Sensitive PII is personal information, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

The Department of Homeland Security (DHS) lists sensitive PII as follows:

Stand alone	In combination with other PII elements
Social Security Number (SSN)	Citizenship and immigration status
Driver’s license or state ID numbers	Personal email, address, and account passwords
Passport number	Medical information
Alien registration number	Ethnic or religious affiliation
Financial account numbers	The last four digits of the SSN
Biometric identifiers	Date of birth
	Criminal history
	Mother’s maiden name

Non-sensitive PII is personal data that is not expected to cause significant harm to the impacted individuals in the event of a privacy breach.

For example, the U.S. National Archives considers a business card or public telephone directory of agency employees as a non-sensitive PII.

The IT industry (IBM Technology Company) considers non-sensitive PII:

- A person's full name, social media account name
- Mother's maiden name
- Telephone number
- IP address
- Place and date of birth
- Geographical details (ZIP code, city, state, country, etc.)
- Employment information
- Email address or mailing address.

Non-Sensitive PII Can Also be Harmful

Please note: Sensitive PII requires more robust and stringent protection. However, it does not mean that non-sensitive PII can be just ignored. PII elements that appear non-sensitive at first glance can become harmful depending on where or in what context they are used. For example:

Mother's maiden name

👍 is not sensitive as a standalone PII element.

👎 is sensitive when used for identity confirmation in online accounts.

A person's full name

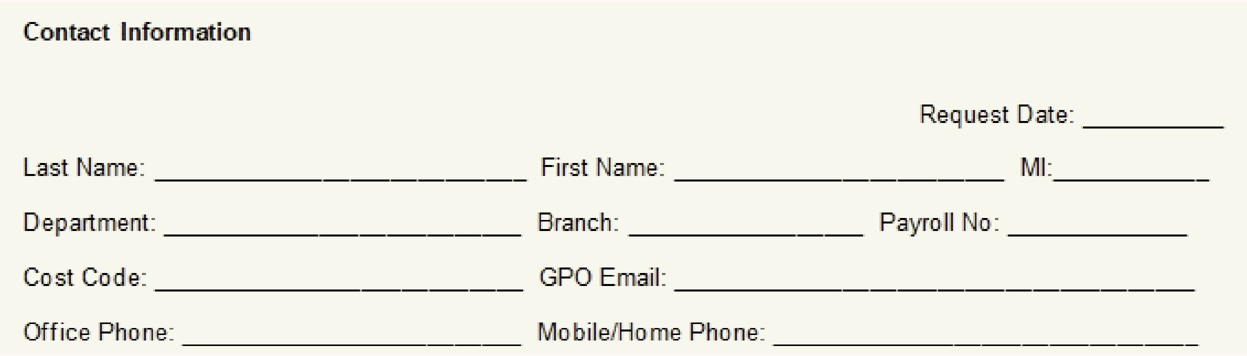
👍 is not sensitive in a list of attendees at a public meeting,

👎 is sensitive in the list of employee performance ratings, law enforcement investigators, or hospital patients.

If you have any questions regarding the level of sensitivity of a PII element you engage, contact the PO (privacy@gpo.gov) or the Business Unit's (BU's) Privacy Point of Contacts (PPOC). If the PO or PPOCs are not accessible, handle suspected PII elements as a sensitive PII.

Case Study 2: PII in business documents

Here, we see the snip of the GPO remote access user information (Figure 2).
If the blanks were filled in, do you think unauthorized disclosure of this document could harm individuals?



Contact Information

Request Date: __________

Last Name: ________________________ First Name: ______________________ MI:__________

Department: _______________________ Branch: _______________ Payroll No: ____________

Cost Code: ________________________ GPO Email: __________________________________

Office Phone: ______________________ Mobile/Home Phone: ____________________________

Figure 2. GPO Remote access user information.

Go to the Case Study Explanations page *(CTRL+ left mouse clicks)* to see our version of the answer to this question.

Consequences of Unauthorized Disclosure of Sensitive PII

Cybercriminals often sell PII elements on the dark web for only a few dollars. Such data may be used for purposes like targeted advertising; however, the potential harm to affected individuals can be much more severe in some cases. Below is an overview of the potential harm of privacy incidents to an impacted individual and to the organizations who are obliged to protect these personal data:

Possible harms for impacted individuals:

- Identity theft, including medical identity theft.
- Financial, tax fraud, damage to credit scores.
- Emotional distress and reputational damage.
- Discrimination, stalking, harassment, blackmail, extortion attempts, or even physical harm.
- Loss of privacy and autonomy.
- Unauthorized access to personal accounts.
- Exposure to social engineering attacks.
- Phishing scams targeting affected individuals.
- Loss of employment opportunities or harm to professional relationships.
- Breaches of health-related information leading to significant physical, emotional, and financial effects.
- Unauthorized use of government services, such as tax benefits, healthcare, or welfare programs.
- Exposed information such as home addresses or travel plans could make individuals more vulnerable to physical threats.

Possible damages to the organization responsible for protecting PII:

- Legal consequences and financial penalties for non-compliance with data protection regulations.
- Reputational damage and loss of customer trust.
- Increased costs for breach mitigation and security improvements.

The price of "Fullz," a term referring to a full set of credentials (SSN, name, DOB, etc.) on the dark web.

Country	Average "Fullz" price
USA	$8
UK	$14
Turkiye	$14
Israel	$14
China	$15
Singapore	$15
Canada	$15
Australia	$15
UAE	$25
Japan	$25
EU	$25

Source: Comparitech, August 12, 2023.

Our PII is at Risk All the Time…

In early 2024, **National Public Data**, a Florida-based online background check and fraud prevention service, experienced a significant data breach. This breach allegedly exposed highly sensitive personal data, including:

- Full names,
- SSNs
- Mailing addresses
- Email addresses
- Phone numbers

Bloomberg Law estimates that about *170 million* people in the US, UK, and Canada were impacted.

In May 2024, **Ticketmaster**, online platform to buy and sell tickets for concerts, sports, theater, family, and other events, reported about a massive privacy incident.

According to an official statement from the company, third-party cloud data services were compromised. The following customer data from North America (U.S., Canada, and/or Mexico) were compromised:

- Email
- Phone number
- Encrypted credit card information

The New York Times reports a hacker group claimed to have stolen data from over *500 million* Ticketmaster customers.

Cost of cybercrime

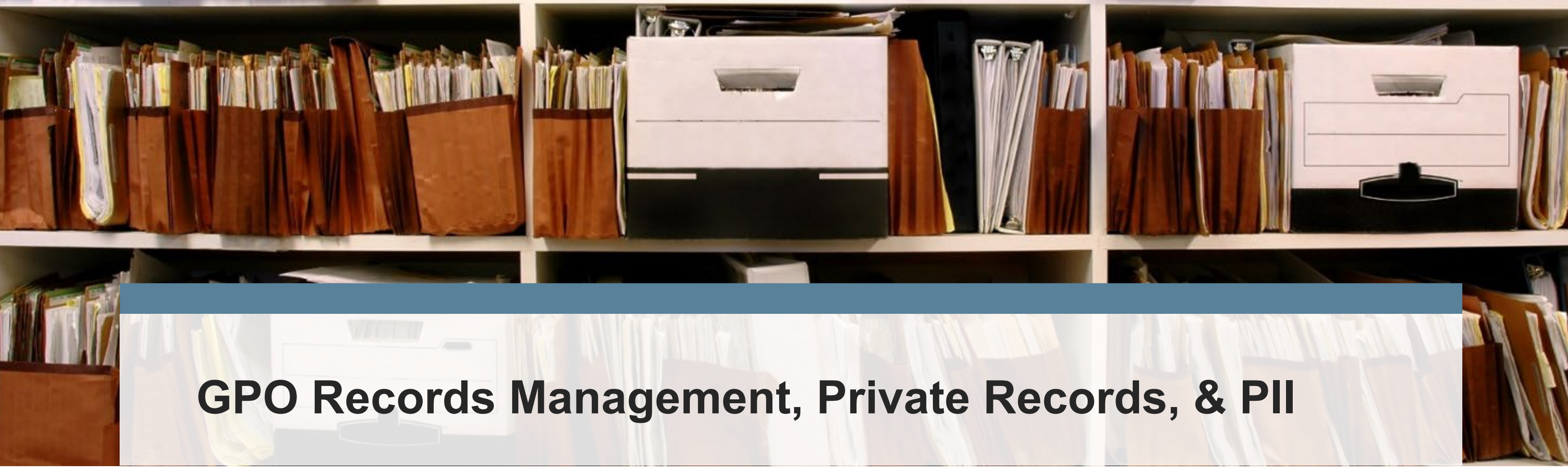
According to Statista, the EU's largest data company, the estimated cost of cybercrime worldwide has increased for eleven consecutive years and is forecasted to reach $15.63 trillion in 2029.

Just for comparison, the total spending of the U.S. Federal Government in FY 2024 was $6.7 trillion.

In February 2024, Change Healthcare experienced a significant data breach. According to the HIPAA Journal, this ransomware attack affected *100 million* individuals, making it the most significant reported data breach in the United States.

The compromised personal information included:

- Health insurance details
- Health information (such as diagnoses, medicines, test results, images, care, and treatment)
- Financial and banking information
- Social Security numbers
- Driver's licenses
- State ID numbers
- Passport numbers



GPO Records Management, Private Records, & PII

GPO records (electronic or paper) can also contain PII or PHI.

GPO’s commitment to privacy extends to the GPO Records Management Program (RMP), encompassing records in all formats and locations, including:

- Possession of Business Units
- Records Management warehouse
- Records’ expungement area

The GPO Privacy Office, in close collaboration with RMP, ensures that safeguards are in place to protect PII in both electronic and paper records.

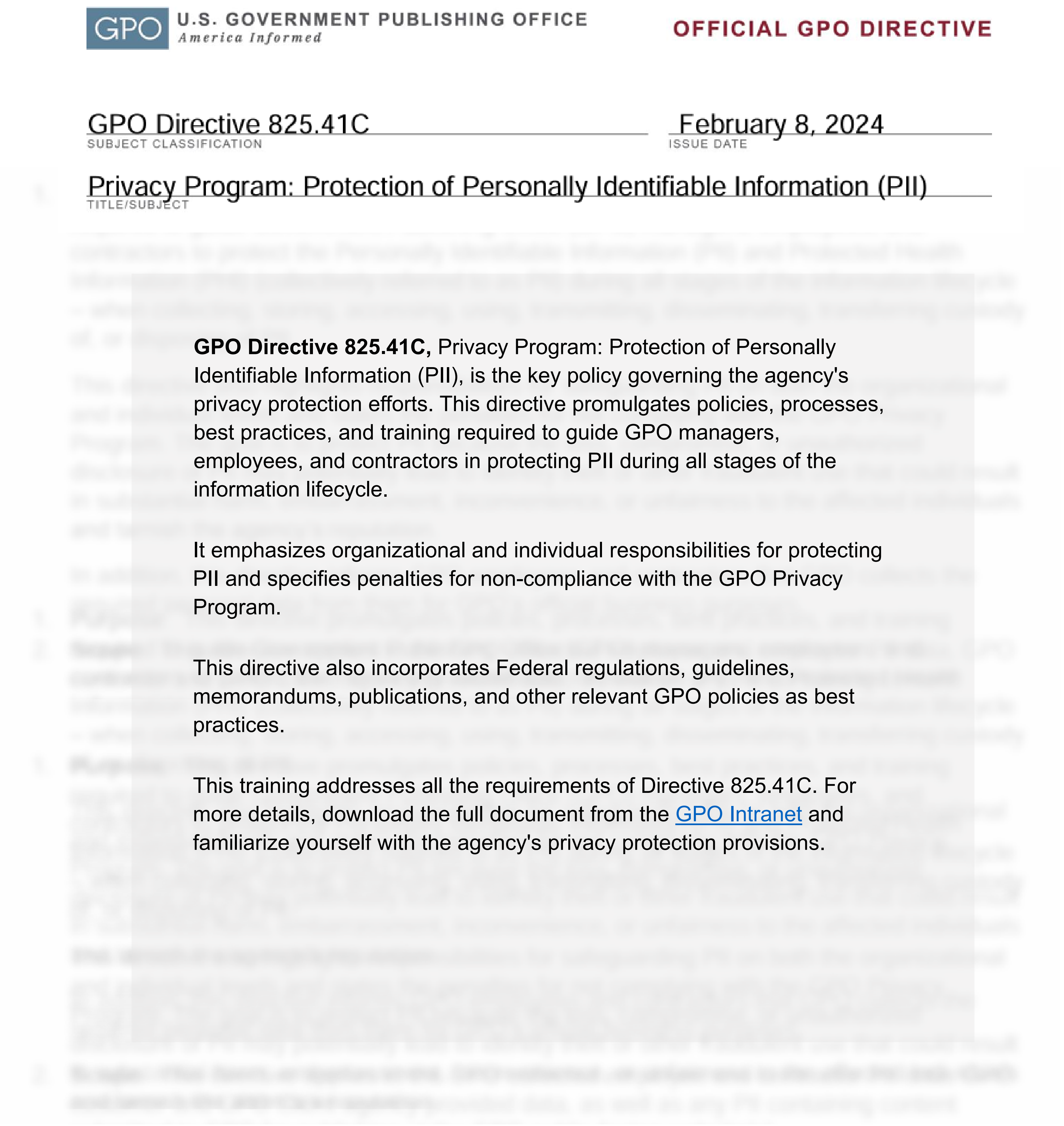
GPO Email as a Private Record

Emails may also be treated as private records when they contain:

- Personal, health, financial, or sensitive information belonging to GPO employees or contractors.
- Other sensitive business information.

Emails are considered records when they create, transmit, receive, or maintain GPO business information electronically. If your role involves maintaining GPO personal or private records, contact the GPO Records Officer or your immediate supervisor for guidance.

Note: The content of the record is what matters—whether it is in paper or electronic format is irrelevant.



GPO U.S. GOVERNMENT PUBLISHING OFFICE *America Informed*

OFFICIAL GPO DIRECTIVE

GPO Directive 825.41C
SUBJECT CLASSIFICATION

February 8, 2024
ISSUE DATE

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

GPO Directive 825.41C, Privacy Program: Protection of Personally Identifiable Information (PII), is the key policy governing the agency's privacy protection efforts. This directive promulgates policies, processes, best practices, and training required to guide GPO managers, employees, and contractors in protecting PII during all stages of the information lifecycle.

It emphasizes organizational and individual responsibilities for protecting PII and specifies penalties for non-compliance with the GPO Privacy Program.

This directive also incorporates Federal regulations, guidelines, memorandums, publications, and other relevant GPO policies as best practices.

This training addresses all the requirements of Directive 825.41C. For more details, download the full document from the GPO Intranet and familiarize yourself with the agency's privacy protection provisions.

Essentials Of PII Safeguarding

For more comprehensive list of PII safeguarding measures, look at the *Safeguarding PII (102) training module* (available on the Privacy page on the GPO Intranet).

Handling of sensitive PII:

- Mark sensitive PII as “Sensitive PII” and label it “For Official Use Only.”
- Retain sensitive PII only as long as necessary. Keep it encrypted and ensure access is controlled. Store hard copies securely in a locked area when not used.
- Never send sensitive PII to personal email accounts. Share it only with authorized people who “need to know.” Encrypt PII-containing emails before sending them internally and externally. Use the GPO-implemented email encryption solution. Avoid sharing passwords through voicemail.
- Do not post sensitive PII on the GPdO Intranet, the Internet (including social media), shared drives, or multi-access calendars accessible to unauthorized individuals.
- Transport sensitive PII physically only between approved locations and with prior authorizations.
- Use an opaque container using First Class, Priority Mail, or a traceable commercial delivery service like UPS, the USPS, or FedEx.
- Dispose of sensitive PII, including archived emails, when it is no longer needed in accordance with the applicable records disposition schedules.
- When retiring, disposing of, transferring ownership, or repairing devices containing PII, GPO IT Operations ensures that all PII on the equipment is permanently irretrievable.
- Refrain from faxing sensitive PII whenever possible. If faxing is unavoidable, contact the recipient directly to confirm receipt, and always include a cover sheet.
- If a device containing PII is lost or stolen, report it immediately as a privacy incident. Follow the instructions in the Incident Reporting section (refer to page 17). The Privacy Office, in collaboration with IT Operations, will take immediate containment measures, which may include remotely locking the device and erasing sensitive data.
- Paper records containing PII (whether your own or others’) that have reached the end of their retention period or have been approved for destruction by a supervisor must be shredded at a GPO-approved shredding facility (GPO Directive 840.1C). The shredding process must be witnessed by a federal employee or an authorized contractor.

Think about privacy when using computers and smart devices (Whether you are working from the GPO office or home, follow these best practices to protect privacy:

- Always lock your computer (Ctrl+Alt+Del, then select “Lock”) when stepping away, even for a few minutes.
- Ensure you log off your computer completely after work.
- Always divert your computer screen from the public eye.
- Don’t download PII on an external storage device not provided by the GPO. Use only GPO-approved portable electronic devices and ensure all PII data is encrypted on them.
- When sharing your screen in applications such as Microsoft Teams, Zoom, or Webex, be cautious of visible sensitive information. It is also good practice to ask for permission before recording online meetings or conferences.

Essentials of PII Safeguarding *(Continued)*

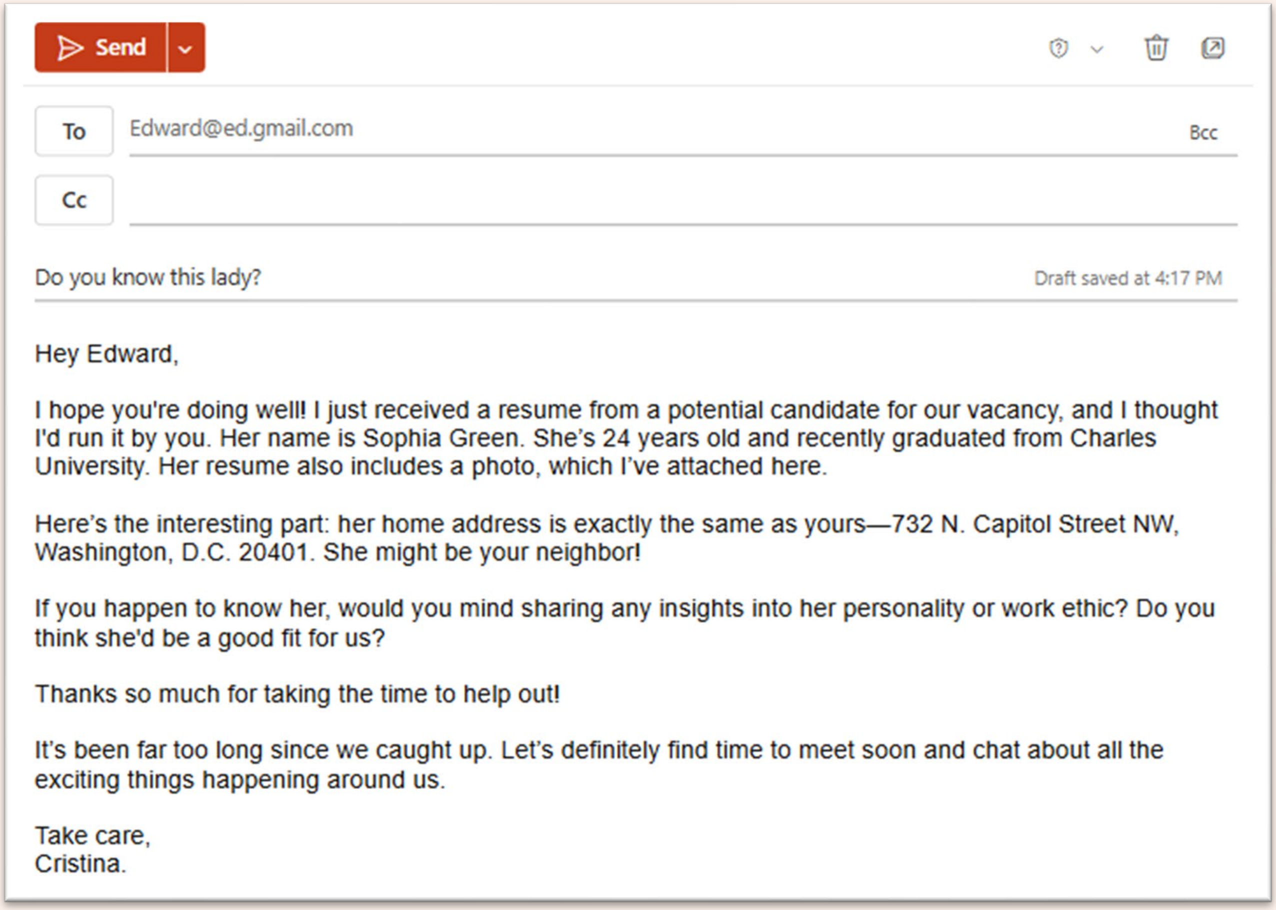
Follow the cyber-hygiene principles:

- Create complex passwords with a mix of letters, numbers, and symbols. Always protect your GPO login credentials (e.g., username and password).
- Whenever available, use two-factor authentication for an extra layer of security.
- Regularly update software and systems to ensure vulnerabilities are patched.
- Avoid clicking on suspicious links or downloading attachments from unknown senders. Stay vigilant against phishing attempts designed to steal sensitive information.
- Be mindful of the personal information you share online, especially on social media and other public platforms.
- Continuously educate yourself about emerging cyber threats and learn how to identify and respond to them.

Case Study 3: PII in the email

Please review the snipped email below. (*Note that all the data used in this fictitious letter are not real information. This is just an imaginary example for training purposes.*) The email contains many PII elements. Can you identify two more major policy violations related to privacy safeguarding?

Go to the Case Study Explanations page to see our version of the answer to this question.



Edward@ed.gmail.com

Do you know this lady?

Draft saved at 4:17 PM

Hey Edward,

I hope you're doing well! I just received a resume from a potential candidate for our vacancy, and I thought I'd run it by you. Her name is Sophia Green. She's 24 years old and recently graduated from Charles University. Her resume also includes a photo, which I've attached here.

Here's the interesting part: her home address is exactly the same as yours—732 N. Capitol Street NW, Washington, D.C. 20401. She might be your neighbor!

If you happen to know her, would you mind sharing any insights into her personality or work ethic? Do you think she'd be a good fit for us?

Thanks so much for taking the time to help out!

It's been far too long since we caught up. Let's definitely find time to meet soon and chat about all the exciting things happening around us.

Take care,
Cristina.

Typical Privacy Incidents

According to *OMB* *M 17-12*, the following scenarios illustrate typical privacy breaches:

- Loss or theft of a laptop or portable storage device containing PII.
- Inadvertently sending an email with PII to the wrong person.
- Misplacing or losing a box of documents with PII during shipping.
- Unauthorized individuals overhearing discussions about an individual's PII.
- Authorized users improperly sell or share PII for personal gain or to embarrass someone.
- Malicious actors gaining access to IT systems that store PII.
- Unintentional public posting of sensitive PII on a website.

In addition to the OBM list above, the International Association of Privacy Professionals (IAPP) lists employee behaviors leading to privacy incidents as follows:

1. **Being overly helpful.** Employees may share unnecessary information to assist clients, increasing the risk of privacy breaches.
2. **Unsecured transmission.** In a rush, employees may transmit data without encryption or adequate protection.
3. **Multi-tasking.** Working with multiple open system windows can lead to entering or transmitting information in the wrong context.
4. **Over-collection of data.** Employees might overlook privacy requirements and collect excessive or unnecessary data.
5. **Inconsistent business processes.** Business changes may neglect privacy policy updates or notifications, exposing organizations to legal risks.

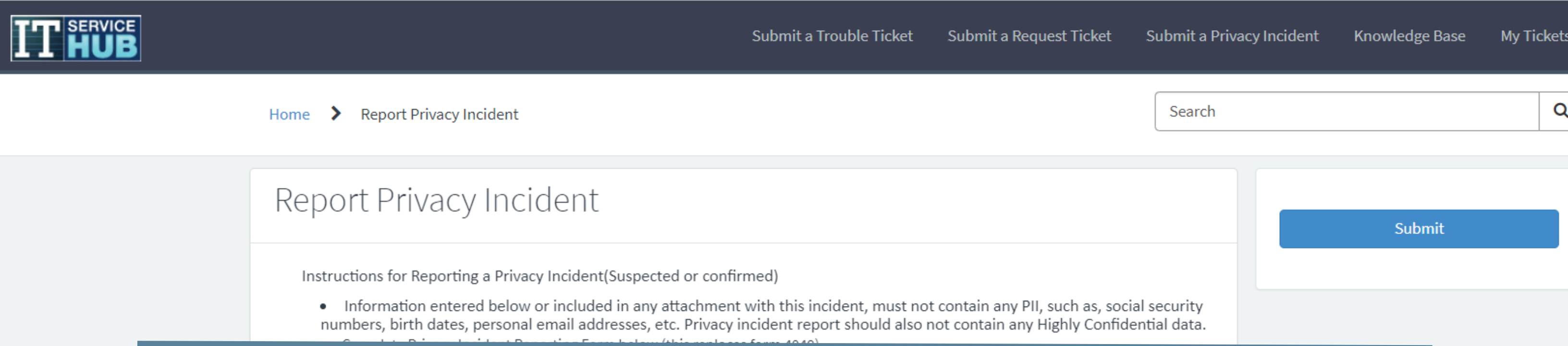
Possible Privacy Incidents scenarios for the GPO

WHAT CAN YOU ADD TO THIS LIST?

Please provide your comments and ideas in your comments section on page 26.

A non-exhaustive list of *possible* privacy incident scenarios for the GPO business process:

- Distributing (intentionally or unintentionally) or receiving PII-containing email or hard copy documents to internal or external recipients.
- Sending PII-containing documents without encryption.
- Posting unredacted PII on GPO Intranet or public-facing website.
- Unauthorized access to the PII-containing data sources (GPO/Cloud/Hosted).
- Breach of GPO customer provided PII at GPO or contractor facility during shipment, electronic transfer, etc.
- Creating recall rosters with SSNs.
- Posting/saving PII-containing documents to shared drives, including SharePoint, MS Teams, and other communication tools.
- Sharing screen displaying PII in conferencing (MS Teams, Zoom, Webex, etc.), particularly when being recorded.
- Leaving hard copy documents containing PII on GPO copy machines and printers.
- Phishing, pretexting, or other social engineering tactics tricking employees/contractors into disclosing PII or providing unauthorized access to secure systems.
- Collecting/storing PII in an unsecured location (e.g., an unencrypted server or unlocked physical document storage).
- Loss or theft of devices containing PII.
- Improper disposal or removal of PII-containing devices such as Multifunctional Devices (MFD) (Printer/Scanner/Fax) hard drives or local storage.
- Thrown away PII-containing documents in regular trash bins rather than being shredded or properly disposed of.
- Improper disposal of PII-containing defective print materials.



Report Privacy Incident

Instructions for Reporting a Privacy Incident(Suspected or confirmed)

- Information entered below or included in any attachment with this incident, must not contain any PII, such as, social security numbers, birth dates, personal email addresses, etc. Privacy incident report should also not contain any Highly Confidential data.

Reporting Privacy Incidents

Under GPO Privacy Directive 825.41C, all actual or suspected privacy incidents must be reported promptly. Reports should be submitted via the Online Privacy Incident Reporting Form (OPIRF), accessible through the IT Service Hub on the GPO Intranet.

The Privacy Office and Privacy Incident Response Team (PIRT) will manage the response using the GPO Privacy Incident Handling Guidance (PIHG). These protocols outline procedures for:

- Risk containment.
- Harm assessment.
- Mitigation measures.

The goal is to minimize harm to impacted individuals and the GPO.

When reporting privacy incidents:

- Provide as much detailed information as possible.
- Include supporting materials, such as documents, webpage URLs, or system process details related to the incident.

For more information, refer to the Standard Operating Procedure (SOP): “Reporting a Privacy Incident.”

GPO Directive 825.41C guides:

#1 Immediately notify your supervisor. Also, contact your BU manager or Privacy Point of Contact (PPOC) at your BU.

#2 Access the GPO Online Privacy Incident Reporting Form (OPIRF) available at the GPO Intranet website.

AI Adds Another Layer of Complexity

Photo: N. Hanacek/NIST

Artificial Intelligence (AI) tools, such as image recognition, speech-to-text, cognitive knowledge platforms, ChatGPT, and many more, can enhance efficiency by automating processes and simplifying tasks. However, they also present unique challenges to privacy:

Collecting sensitive PII data using AI tools or putting PII data into AI tools' databases may broaden PII exposure, potentially resulting in additional PII incidents.

AI can also cause another challenge: exercising the privacy principle of the individual's right to update or remove personal information, which becomes more difficult with AI because the data may have crossed the GPO systems' boundaries. Always ensure that PII is protected from accidental inclusion in AI Learning Models and related issues.

For more information, please visit the GPO AI initiatives on the GPO Intranet.

Case Study 4: Reporting privacy incident

Alice and Alex meet in the cafeteria

Please note:

the scenario and the sample letter provided are entirely fictional.
They are only examples created for the purpose of this training.

Alice: *Hey, I need to talk to you about something.*

Alex: *Sure! What's up?*

Alice: *I found this paper on the floor in the hall on my way here. I'm not sure what to do with it. Can you look and check if it's important?*

Alex: *Let me see... Hmm, this is an old document from our agency that was sent to employees a few years ago. It looks like someone might have dropped it on their way to the trash.*

Alice: *Oh, okay. So, should I just throw it away?*

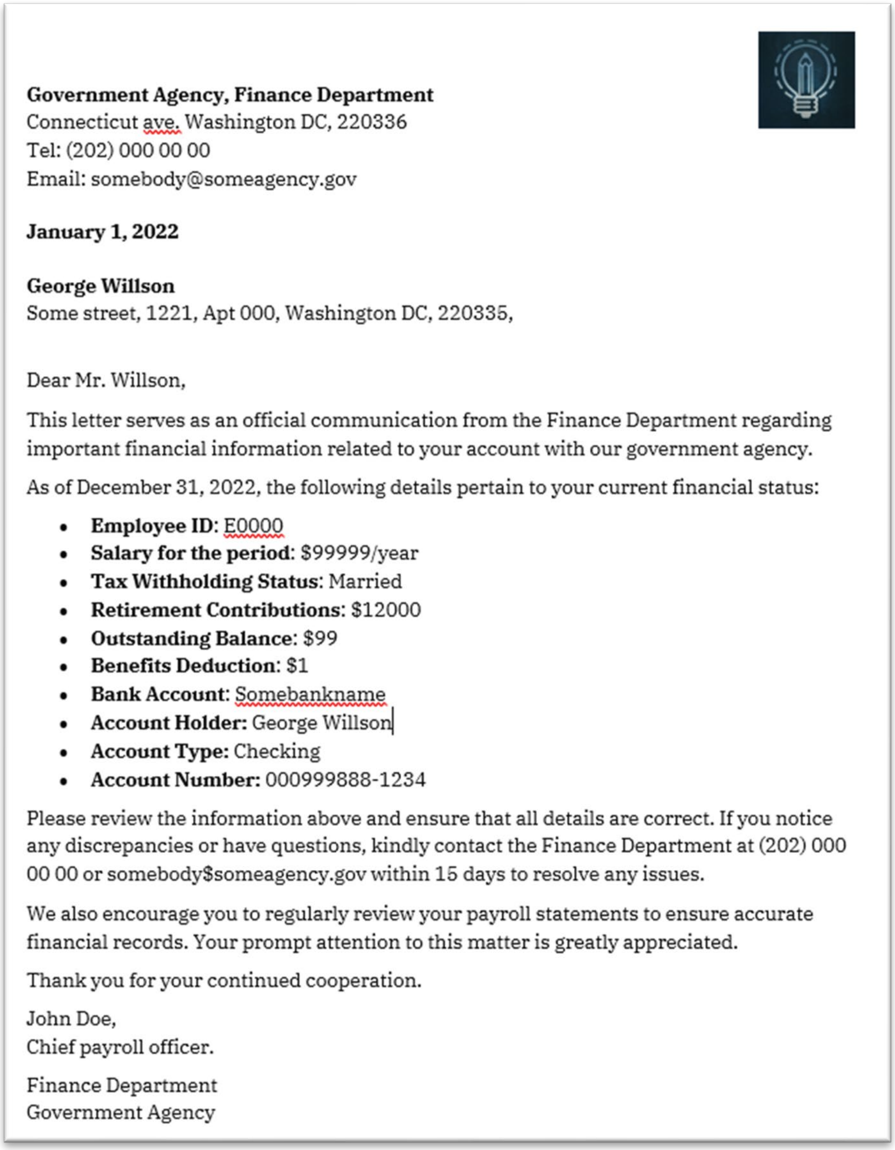
Alex: *Yeah, it's not a problem.*

Alice: *Thanks for checking!*

Alex: *Anytime!*

Think about this scenario and try to find mistakes of both Alice and Alex.

Go to the Case Study Explanations page to see the answer.



Government Agency, Finance Department
Connecticut ave. Washington DC, 220336
Tel: (202) 000 00 00
Email: somebody@someagency.gov

January 1, 2022

George Willson
Some street, 1221, Apt 000, Washington DC, 220335,

Dear Mr. Willson,

This letter serves as an official communication from the Finance Department regarding important financial information related to your account with our government agency.

As of December 31, 2022, the following details pertain to your current financial status:

- **Employee ID**: E0000
- **Salary for the period**: $99999/year
- **Tax Withholding Status**: Married
- **Retirement Contributions**: $12000
- **Outstanding Balance**: $99
- **Benefits Deduction**: $1
- **Bank Account**: Somebankname
- **Account Holder:** George Willson
- **Account Type:** Checking
- **Account Number:** 000999888-1234

Please review the information above and ensure that all details are correct. If you notice any discrepancies or have questions, kindly contact the Finance Department at (202) 000 00 00 or somebody$someagency.gov within 15 days to resolve any issues.

We also encourage you to regularly review your payroll statements to ensure accurate financial records. Your prompt attention to this matter is greatly appreciated.

Thank you for your continued cooperation.

John Doe,
Chief payroll officer.

Finance Department
Government Agency

Corrective & Disciplinary Actions

Records Management Directive 840.1C:

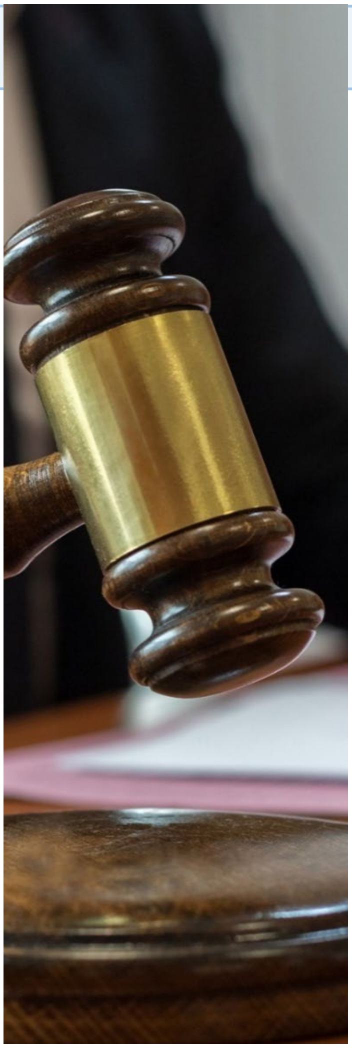
Improper management of records includes:

- Removing, concealing, or altering Federal records.
- Damaging, destroying, deleting, or losing Federal records.
- Disclosing national security information.
- Using Federal records for personal purposes.

Failure to properly manage GPO records could result in criminal penalties.

Potential penalties for the improper management of records include:

- Fine, three years imprisonment, or both.
- Removal from office.
- Disqualification from holding any other office in the Government.

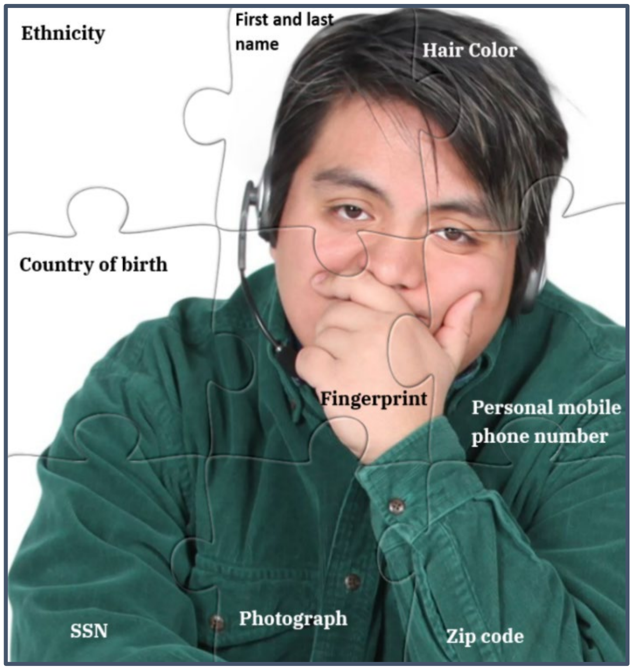


Privacy Directive 825.41C:

Employees and contractors may be subject to disciplinary actions ranging from reprimand to termination (even criminal sanctions and penalties in some cases) for the following proven facts:

- Failing to implement and maintain the established security and safeguarding standards and procedures over PII for which an employee is responsible and aware.
- Exceeding authorized access to or disclosure to unauthorized persons of PII.
- Failing to report privacy-related incidents or breaches for which the employee is responsible or aware.

Case Study Explanations



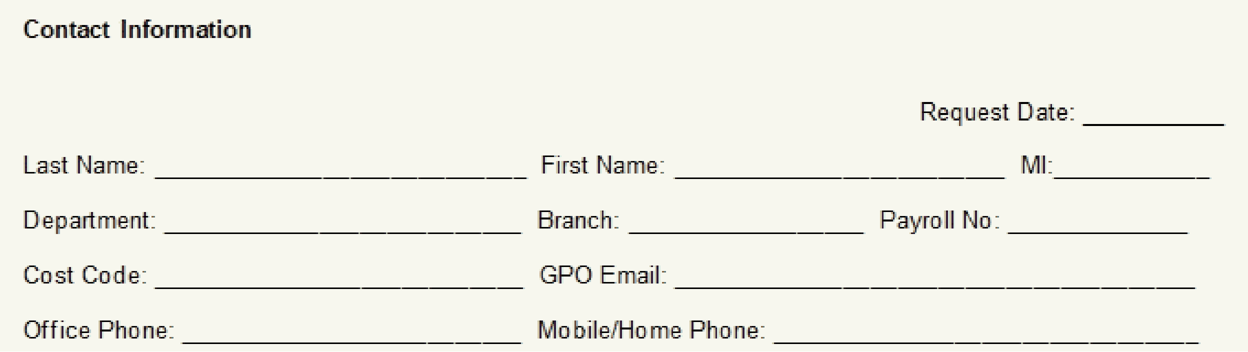
Case Study #1: **Identifiers**
The proliferation of deepfakes and AI technology makes answering this question challenging. For example, nowadays, photographs can be easily altered even with simple mobile applications. With such nuanced cases in mind, we can list direct identifiers from the given puzzle as follows:

1. SSN
2. Fingerprint
3. Personal mobile phone number
4. Photograph (particularly a full-face image)

☞ [Back to study.]()

Case Study #2: PII in business documents.

We must protect this GPO Remote access user information as a PII-containing document. It contains all the information malicious actors need to harm impacted individuals within the agency. For example, this information can help ill-intended individuals send benefits requests, request access to some GPO systems, etc.



Contact Information

Request Date: ___________

Last Name: ___________________________ First Name: ________________________ MI:___________

Department: __________________________ Branch: _________________ Payroll No: _____________

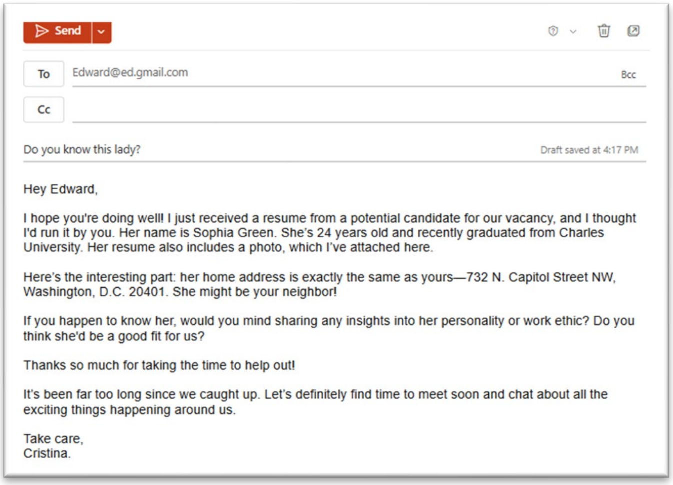
Cost Code: ___________________________ GPO Email: _______________________________________

Office Phone: _________________________ Mobile/Home Phone: _______________________________

Figure 2. GPO Remote access user information.

☞ [Back to study.]()

Case Study Explanations *(Continued)*



To Edward@ed.gmail.com

Cc

Do you know this lady?

Draft saved at 4:17 PM

Hey Edward,

I hope you're doing well! I just received a resume from a potential candidate for our vacancy, and I thought I'd run it by you. Her name is Sophia Green. She's 24 years old and recently graduated from Charles University. Her resume also includes a photo, which I've attached here.

Here's the interesting part: her home address is exactly the same as yours—732 N. Capitol Street NW, Washington, D.C. 20401. She might be your neighbor!

If you happen to know her, would you mind sharing any insights into her personality or work ethic? Do you think she'd be a good fit for us?

Thanks so much for taking the time to help out!

It's been far too long since we caught up. Let's definitely find time to meet soon and chat about all the exciting things happening around us.

Take care,
Cristina.

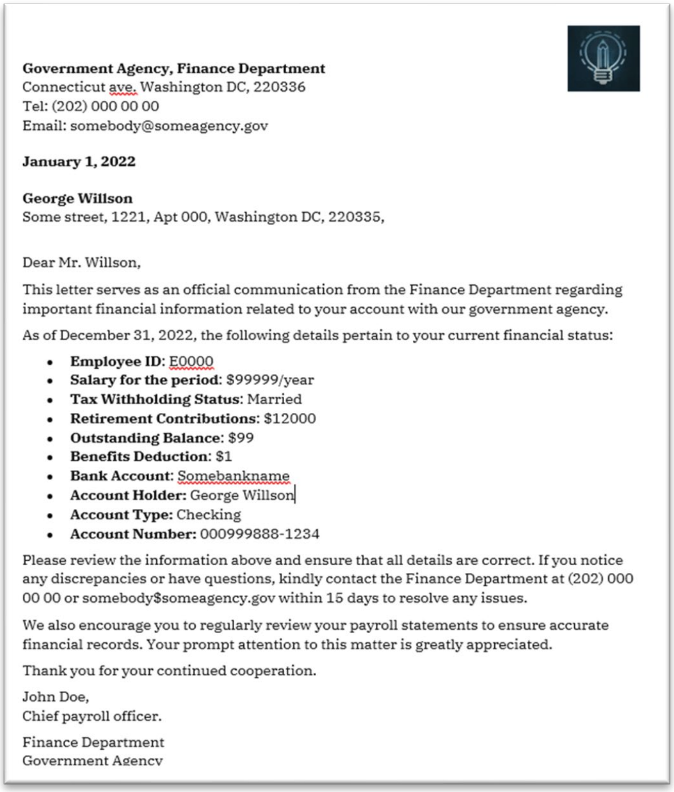
Case Study #3: PII in the email

Policy violations:

1. A PII-containing email was sent outside the GPO. The way background checks are done is also unacceptable. Her neighbors would not be part of a standard background check or consulted unless she provided them as a reference.

2. The email has been sent without adequately encrypted and without a person's permission.

☞ Back to study



Government Agency, Finance Department
Connecticut ave. Washington DC, 220336
Tel: (202) 000 00 00
Email: somebody@someagency.gov

January 1, 2022

George Willson
Some street, 1221, Apt 000, Washington DC, 220335,

Dear Mr. Willson,

This letter serves as an official communication from the Finance Department regarding important financial information related to your account with our government agency.

As of December 31, 2022, the following details pertain to your current financial status:

- **Employee ID**: E0000
- **Salary for the period**: $99999/year
- **Tax Withholding Status**: Married
- **Retirement Contributions**: $12000
- **Outstanding Balance**: $99
- **Benefits Deduction**: $1
- **Bank Account**: Somebankname
- **Account Holder:** George Willson
- **Account Type:** Checking
- **Account Number:** 000999888-1234

Please review the information above and ensure that all details are correct. If you notice any discrepancies or have questions, kindly contact the Finance Department at (202) 000 00 00 or somebody$someagency.gov within 15 days to resolve any issues.

We also encourage you to regularly review your payroll statements to ensure accurate financial records. Your prompt attention to this matter is greatly appreciated.

Thank you for your continued cooperation.

John Doe,
Chief payroll officer.

Finance Department
Government Agency

Case Study #4: Reporting privacy incident

Instead of discussing the PII-containing document with a colleague (which is another layer of unauthorized PII disclosure), Alice should take it immediately to her supervisor. Her supervisor and Alice then discuss future actions, including returning the document to the business unit to which it belongs and reporting this privacy incident.

Alex offered the wrong advice. Any PII-containing documents cannot be thrown into the trash bin regardless of age. Such documents can be accessible by other unauthorized individuals in future steps. Therefore, as the GPO Privacy policy states, all PII-containing hard copy documents must be shredded using GPO-provided guidelines (GPO Directive 840.1C).

☞ Back to study.