

# Information Security—Protecting Sensitive and Classified Information

---

## Identifying Sensitive Information

Sensitive information includes For Official Use Only (FOUO), Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), financial information, personal or payroll information, Protected Health Information (PHI), and operational information. Sensitive information may contain:

- An individual's PII, such as medical (PHI) or financial records
- Information provided by a confidential source (person, commercial business, or foreign government) on condition it would not be released
- Information that could compromise government missions or interests

## Identifying PII and PHI

### Personally Identifiable Information (PII):

- Social security numbers
- Dates and places of birth
- Mothers' maiden names
- Biometric records

### Protected Health Information (PHI):

- Is health information that identifies the individual
- Is a subset of health information, including demographic information
- Is created or received by a healthcare provider, health plan, or employer
- Relates to:
  - Physical or mental health of an individual
  - Provision of healthcare to an individual
  - Payment for the provision of healthcare to an individual

## Data Classification Guidelines—Classified

**Classified data is designated by the original classification authority as:**

- Confidential – information that could reasonably be expected to cause damage to national security if exposed
- Secret – information that could reasonably be expected to cause serious damage to national security if exposed
- Top Secret – information that could reasonably be expected to cause exceptionally grave damage to national security if exposed

**Classified data:**

- Must be handled and stored properly based on classification markings and handling caveats
- Can **only** be accessed by individuals with all of the following:
  - Appropriate clearance
  - Signed, approved non-disclosure agreement
  - Need-to-know

## Data Classification Guidelines—Unclassified

Unclassified is a designation to mark information that does not have potential to damage nation security (that is, it has not been determined to be Confidential, Secret or Top Secret).

**Unclassified data:**

- Must be cleared before being released to the public
- Must be clearly marked as Unclassified, along with any handling caveats, if included in a classified document or storage area
- If aggregated, the classification of the information may be elevated to a higher level of sensitivity
- If compromised, could affect the safety of government personnel, missions, and systems

## **Tips for Protecting Sensitive Information**

- Store sensitive data only on authorized systems
- Don't transmit, store, or process sensitive info on non-sensitive systems
- Handle and store sensitive information properly
  - Reduce risk of access during working hours
  - Store after working hours:
    - Locked or unlocked containers, desks, cabinets, if security is present
    - Locked containers, desks, cabinets if no security is present or is deemed inadequate
- Follow your organization's policy for retention or disposal
- Ensure that all receivers' have required clearance and/or official need-to-know before transmitting sensitive information or using or replying to e-mail distribution lists
- If faxing information:
  - Ensure recipient is at the receiving end
  - Use correct cover sheet
  - Contact the recipient to confirm receipt

## **Tips for Protecting Classified Information**

- Only use data in areas with security appropriate to classification level
- Store classified data appropriately in GSA-approved vault or container when not in use
- Don't assume open storage in a secure facility
- Balance need to share with need to know
- Ensure proper labeling:
  - Appropriately mark all classified material and, when required, sensitive material
  - Report inappropriately marked material
- Never transmit classified information via an unsecure fax machine

## **Tips for Protecting PII and PHI**

- Avoid sharing sensitive information using shared folders or shared applications (such as SharePoint or Google Docs) unless access controls are established that allow only those personnel with an official need-to-know to access the information.
- Follow your organization's policies on the use of mobile computing devices and encryption
- Use only mobile devices approved by your organization
- Encrypt all sensitive data, including PII and PHI, on mobile devices and when e-mailed. The DoD requires two-factor authentication for access.
- Never allow sensitive data on non-government-issued mobile devices.
- Never use personal e-mail accounts for transmitting PII and PHI. PII and PHI may only be e-mailed between government e-mail accounts and must be encrypted and digitally signed when possible.

## Tips for Handling Classified Data on the Internet

If you find classified government data or information not cleared for public release on the Internet:

- Remember that leaked classified or controlled information is still classified or controlled even if it has already been compromised
- Do not download it because you are not allowed to have classified information on your computer and downloading it may create a new case of spillage
- Note any identifying information and the Website's URL
- Report the situation to your security POC
- Never confirm or deny validity of leaked government information

**Remember!** Any comment by you could be treated as official confirmation by a government spokesperson.

## Spillage Tips

Never cross classification boundaries! Do not remove equipment, including mobile devices, from a classified network for use on an unclassified network or a classified network of lower classification, or vice-versa, even if the device's memory has been purged.

Spillage occurs when information is "spilled" from a higher classification or protection level to a lower classification or protection level.

### To prevent inadvertent spillage:

- Be aware of which network you are using
- Be aware of classification markings and all handling caveats
- Follow procedures for transferring data to and from outside agency and non-government networks
- Label all files, removable media, and subject headers

### If spillage occurs:

- Immediately notify your security POC
- Do not delete the suspected files
- Do not forward, read further, or manipulate the file
- Secure the area