# Frequently Asked Questions (FAQ)

1. **What is PII?**

Personally Identifiable Information, or PII, is information that can be used to distinguish, locate, trace, or contact any individual. PII includes any information that may be linked or "linkable" to an individual, such as medical, educational, financial, or employment information. With the increased use of Information Technology (IT) and the Internet, the protection of PII in various forms has become an essential part of protecting individuals from harm associated with unauthorized information disclosure.

**2. What do you mean by "distinguish" an individual?**

To distinguish an individual is to identify and individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data.

**3. What do you mean by "linked or linkable" to an individual?**

Linked information is information about or related to an individual that is logically associated with other information about the individual. For example, if two systems contain different PII elements, and someone has access to both systems, the information may be linked together and associated with the individual. Linkable information within information systems compounds the level of risk associated with maintaining various forms of PII. Linkable information that is not directly associated with an individual (e.g. credit ratings that are not directly associated with the individual)

4. **What are some examples of PII?**

Some example of PII that require protection under the Privacy Act and other Indian Affairs and Department of the Interior policies are:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number (TIN), patient identification number, and financial account or credit card number
- Address or location information, such as street address or e-mail address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face of other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g. retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information

- Information about an individual that is linked to or linkable to one of the above (e.g. date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

**5. How do I determine the level of sensitivity associated with information?**

Assigning sensitivity levels and determining potential or actual impacts associated with disclosure of information including but not limited to PII are the responsibility of the CISO and Privacy Officer. All questions regarding information sensitivity or information handling should be directed to the IA Privacy Officer (contact information below). Some general concepts associated with PII confidentiality impact levels are provided below as a reference. (NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information*)

Determining the impact from a loss of confidentiality of PII should take into account several relevant factors. Firstly, the combination of several types of PII may indicate a higher risk due to the heightened likelihood of identity theft associated with multiple types of PII. Additionally, the following factors must be taken into consideration when assessing the impact of PII disclosure:

a. **Identifiability –** How easily PII can be used to identify specific individuals. For example, PII comprised of individuals' names, fingerprints, or SSNs uniquely and directly identify individuals, whereas PII comprised of individuals' ZIP codes and dates of birth can indirectly identify individuals. Data comprised of only individuals' area codes and gender usually do not provide for direct or indirect identification of an individual depending upon the context and sample size.
b. **Quantity of PII –** PII breaches that vary in size or scope in terms of the number of records or affected individuals may have different impacts, not only in terms of the collective harm to individuals, but also in terms of harm to the organization's reputation and the cost to the organization in addressing the breach.
c. **Data Sensitivity –** Varied forms of PII may have varied levels of sensitivity based on the potential for the information to be used in an unauthorized manner. For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code. Most organizations consider a data set that includes even one SSN to be at least a moderate impact level. Some combinations of PII are more sensitive, such as name and credit card number, than each data fields would be considered without the existence of others. Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use. For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites.
d. **Context –** The context of use factor is related to the Fair Information Practices of Purpose Specification and Use Limitation. Context of use is defined as the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated. Examples of context include, but are not limited to, statistical analysis, eligibility for benefits, administration of benefits, research, tax administration, or law enforcement. For example, suppose that an organization has three lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization. The second list is people who

have filed for retirement benefits, and the third list is individuals who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each of the three lists. Based on the context of use only, the three lists are likely to merit impact levels of low, moderate, and high, respectively.

e. **Obligation to Protect Confidentiality –** Many organizations are subject to laws, regulations, or other mandates governing the obligation to protect personal information, such as the Privacy Act of 1974, OMB memoranda, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Additionally, some Federal Agencies such as the Census Bureau and the Internal Revenue Service (IRS) are subject to additional specific legal obligations to protect certain types of PII. (e.g., Gramm-Leach-Bliley Act – GLBA and Confidential Information Protection and Statistical Efficiency Act – CIPSEA)

f. **Access to and Location of PII –** the access to and location of PII is an important consideration for identifying the potential risks of unauthorized access or release. When PII is access more often by more people and systems, there are more opportunities for the confidentiality of the PII to be compromised.

**6. What do you mean by harm?**

Harm means any adverse or negative effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality or PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability. (NIST SP 800-122)

**7. What is an information owner?**

An information owner, as defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 is the "official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. (CNSSI 4009) Within Indian Affairs, the "Information Owner" role is synonymous with the "Business Owner".

**8. Can I save records containing sensitive information or PII on a portable storage device such as a thumb/flash drive or external hard drive?**

No. Under no circumstances should sensitive information be stored on a portable storage device unless previously authorized by the Bureau Chief Information Security Officer (CISO). The only exception to this prohibition is when such storage is required in support of the organizations mission, the storage device is Government furnished, the information is reviewed and approved by the CISO or IA Privacy Officer prior to storage, and the portable device is encrypted using a Federal Information Processing Standards (FIPS) Publication 140-2 (as amended) validated cryptographic module.

Under no circumstances may employees or contractors store any Government information (sensitive or non-sensitive) on personnal owned equipment of any kind. Non-government owned portable devices shall not be connected to DOI/BIA systems at any time for any reason.

**9. What is a record?**

The term "record" means nay item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph.

**10. What are sanctions?**

Sanctions are disciplinary and adverse actions that may be taken by management officials in the event that and employee intentionally or unintentionally disregards, circumvents, or disobeys organizational policies and procedures. Personnel are responsible for protecting the confidentiality, availability, and integrity of data and information accessed, stored, processed, and transmitted. Individuals are accountable for actions taken on and with IA and BIA IT information resources. Unauthorized disclosure of sensitive information including but not limited to PII may also result in criminal or civil penalties.

For the purpose of defining sanctions related to the unauthorized disclosure of sensitive or PII, the following excerpt from the Departmental Manual (DM) Part 370 Chapter 752 Appendix B is included herein. For a complete listing of Discipline and Adverse Actions, see the DM Part 370 Chapter 752 here: http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3738

| Nature of Offense | Penalty for First Offense | Penalty for Second Offense | Penalty for Third Offense |
|---|---|---|---|
| **Information is not compromised and release is unintentional** | Written Reprimand to 5-day suspension | 5- to 30-day suspension | 30-day suspension |
| **Information is compromised and release is unintentional** | Written Reprimand to 30-day suspension | 30-day suspension to removal | Removal |
| **Release of restricted information is deliberate** | 30-day suspension to removal | Removal | |

**Departmental Manual Part 370 Chapter 752.1**

11. **What is a PII incident or event?**

Any form of suspected or confirmed disclosure of PII. Regardless of context or information type, all disclosures of PII must be reported to and reviewed by the IA Privacy Officer.

12. **How do I report a suspected or confirmed disclosure of sensitive information?**
    a. Privacy Loss Mitigation Strategy
    b. PII Incident Handling Process (incorporate details from Randy)
    c. Integrate process with CIRT processes, Messaging processes, Systems processes, etc.
    d. Discuss process with HR to obtain guidance (acceptable use provisions, sanctions, etc.)

For questions regarding the Departmental Privacy Program, please contact the Indian Affairs Privacy Officer:

Willie S. Chism, CIPP/G
Division of Privacy and Records
Office of Information Security and Privacy
625 Herndon Parkway
Herndon, VA 20170
(o) 703-735-4163
(f) 703-735-4164
Willie.Chism@bia.gov

A full listing of Privacy points of contact within DOI can be found here:
http://www.doi.gov/archive/ocio/privacy/doi_privacy_act_officers.htm

# List of Published Resources and Links

1. DOI Privacy Program - http://www.doi.gov/archive/ocio/privacy/
    a. Subject Index for Department of the Interior (DOI) Privacy Act Regulations and the Privacy Act Manual Sections
    b. DOI Regulations for Implementing the Privacy Act
    c. DOI Manual Sections on the Privacy Act (383 DM 1-15)
    d. DOI Bureau Program Responsibilities (383 DM 3)
    e. DOI Privacy Act System of Records Notices and Government-wide Notices
    f. DOI Privacy Act Regulations on Contracts (43 CFR 2.53)
    g. DOI Web site Privacy Policy
    h. DOI Privacy Policy for the Information Sharing Environment
2. Government – Links to Federal Privacy Act Resources:
    a. The Privacy Act of 1974, as amended (5 U.S.C. 552a)
    b. A Citizens Guide to the FOIA and Privacy Act
    c. Privacy Provisions of the E-Government Act of 2002
    d. Office of Management and Budget (OMB) Privacy Policy Guidance
    e. OMB Circular A-130, Management of Federal Information Resources
3. Reference Materials
    a. Privacy Act System of Records Notices and Preparing Notices
    b. Privacy Impact Assessments
    c. Privacy Protection Tips
    d. Policies on Safeguarding Personally Identifiable Information (PII) and Social Security Numbers
4. Privacy Act System of Records Notices and Preparing Notices
    a. DOI Privacy Act System of Records Notices and Government-wide Notices
    b. DOI Manual Chapter on Privacy Act System of Records Notices (383 DM 5)
    c. Government Printing Office Drafting Handbook

d. Indian Affairs System of Records Notices - http://www.doi.gov/archive/ocio/privacy/bia_notices.htm

e. DOI and Government-wide Systems of Records - http://www.doi.gov/archive/ocio/privacy/List_doipa_notices_9-06-06.html

5. Privacy Impact Assessments
   a. OCIO Bulletin 2002-015, Privacy Impact Assessments for Department of the Interior Information Systems
   b. DOI Privacy Impact Assessment and Guide
   c. PowerPoint on the Basics of the Privacy Impact Assessment
   d. Privacy Impact Assessment Template
   e. Public Privacy Impact Assessments - http://www.doi.gov/archive/ocio/privacy/ppia.html
6. Privacy Protection Tips
   a. President's Task Force on Identity Theft
   b. Federal Trade Commission (FTC) Privacy Initiatives
   c. FTC's "Fighting Back Against Identity Theft" Site
7. Policies on Safeguarding Personally Identifiable Information
   a. Office of Personnel Management Memorandum, Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft (June 18, 2007)
   b. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
   c. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information
   d. OMB Memorandum M-06-16, Protection of Sensitive Agency Information
8. Departmental Manual (DM) Part 370 Chapter 752 – Discipline and Adverse Actions http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3738