UNDERSTANDING PII GUIDEBOOK

WHAT IS PII?

Personally Identifiable Information (PII) is any data that can be used to **directly or indirectly identify** a specific individual.

Navigating personal information privacy has become increasingly complex in an era of widespread social media and professional networking. While individuals routinely share significant personal details on platforms like Facebook and LinkedIn—revealing birthdays, employers, locations, and life milestones—agencies still bear a critical legal and ethical responsibility to protect this information.

TYPES OF PII

Personally Identifiable Information (PII) can be categorized into sensitive and non-sensitive types based on the potential for harm if disclosed. **Sensitive PII** includes information that can directly enable identity theft, fraud, or personal harm, such as Social Security numbers, financial account details, medical records, and precise location data. These types of information require strict protection because they can be used to compromise an individual's privacy, financial security, or personal safety.

In contrast, **non-sensitive PII** involves information that poses minimal risk if shared publicly, such as general professional titles, public directory listings, or broad demographic information. The critical distinction is that the sensitivity of PII is not inherent to the information itself, but depends entirely on **the context, purpose, and potential consequences** of its disclosure. What might be considered harmless in one scenario could become a significant privacy risk in another, making careful evaluation of information sharing essential for protecting personal data.

PII	SENSITIVE PII
Full Name	Social Security Number (SSN)
Date of Birth	Driver's License Number
Email Address	Passport Number
Phone Number (Especially Mobile)	Financial Account Information:
Home Address (Partial)	Bank account numbers
Employment Information:	Credit card numbers
Job title	Debit card numbers
Employer name	Account passwords
School names	Diagnoses
Degrees earned	Treatment history
Username/User ID	Prescriptions
IP Address	Genetic information
Online Identifiers (e.g., social media handles)	Fingerprints
	Facial recognition data
	DNA
	Precise GPS coordinates
	Home address

Contact ODGA’s Data Protection and Governance Team for assistance.

EXAMPLES

Context is key when determining if the PII you have is sensitive.

- **Context:** How might this information be misused?
- **Purpose:** Why is the information being shared?
- **Potential Harm**: Could sharing cause personal risk? Even seemingly "less sensitive" data can become highly sensitive when combined with other information.

For example, the sensitivity of data elements like name or address can change based on the context.

PII	Sensitive	Non-Sensitive
Names	• Full name linked to specific medical conditions • Reveals personal health details • Names in criminal investigations • Victim or witness identification • Pending legal proceedings • Government assistance programs • Personal economic vulnerabilities	• Team sports rosters • Professional achievement announcements • Public event participant lists • Company employee rosters • Academic faculty listings • Standard business communications • General customer service
Home Address	• Victim protection records • Child support or custody documents • Confidential government employee locations • Domestic violence survivor information	• Public voter registration lists • Business licensing records • Professional mailing directories
Phone Number	• Associated with personal accounts • Used for two-factor authentication • Linked to private communication records	• Public business contact information • Professional directory listings • General customer service interactions
Email Addresses	• Contains full name or personal identifier • Connected to multiple personal accounts • Used for identity verification	• Professional communication • Public event registrations • Standard newsletter subscriptions
Date of birth	• Medical records identifying patient age and risk factors • Financial applications revealing exact age • Background checks with complete birth date	• Public recognition (e.g., team birthdays) • Generic demographic studies • Professional biographical summaries without full date
IP Addresses	• Linked to specific user's online activities • Reveals precise geographic location • Connected to personal browsing history	• Generic network monitoring • Public Wi-Fi usage tracking • Broad statistical analysis
Employer Name	• Whistleblower protection cases • Confidential government positions • Employees in high-risk occupations • Sensitive military or intelligence roles	• Standard professional networking • Public employee directories • Industry conference participant lists

Contact ODGA's Data Protection and Governance Team for assistance.