🔒 Privacy Basics: Information Sheet for Employees

This guide explains the fundamental concepts of privacy and what your duties are when handling personal information.

What is Personal Information?

Term	Definition
Privacy	Your fundamental duty to handle data respectfully, securely, and transparently. It is the right of individuals to control how their personal details are collected and used.
Personal Information (PII/PI)	Any recorded detail that can be used to **identify a specific person**. This is the information you must protect.
Examples of PII	**Obvious:** Name, home address, personal phone number, financial information, health history, fingerprints (biometric information). **Less Obvious:** Educational history, opinions about an individual, employment history, or an identifying number assigned to a person.

The Data Lifecycle: Rules for Handling PII

Before you deal with any personal information (PII), the organization must have a legal reason to do so. This is called **Authority**.

Action	Definition	Rule for Employees
Authority	The **legal permission** the organization must have (usually from a specific law) before it can collect, use, or share PII. Without Authority, handling the data is illegal.	If you are unsure if your action is authorized, **ask your Privacy Officer or supervisor** before proceeding.
Collection	When the organization **gathers or receives** PII.	You must generally collect information **directly from the individual** it is about. Only collect the **minimum amount** of PII that is directly necessary for your specific, authorized program or activity.
Use	The ways the organization **handles or processes** the PII internally (e.g., running a program, providing a service, or making a decision).	The data can only be used for **the original reason it was collected**, or for a purpose that is **directly and logically connected** to that original reason ("consistent purpose").

Disclosure	When the organization **shares or gives** PII to another person, system, or organization. This can be oral (speaking) or in writing (email, paper).	You can only disclose PII if the law **explicitly authorizes** the sharing. You must only disclose the **minimum amount** of PII necessary to achieve the authorized purpose.

Employee Access and Protection Standards

1. When Employees Should Access PII

All employees are required to protect the information under their control. Your access to PII is strictly limited by the "**need-to-know**" principle:

- You may only look at, use, or access PII **if it is absolutely necessary to perform your specific, authorized job duties**.
- If you access PII for curiosity, personal reasons, or any purpose that is not essential to your current task, this is considered **unauthorized access** (sometimes called "snooping"). Unauthorized access is a serious privacy breach.

2. Reasonable Security Arrangements

Your organization must maintain **Reasonable Security Arrangements**—protective measures that are appropriate for the sensitivity of the data—to keep PII safe from unauthorized access, use, or destruction.

These security arrangements include three types of safeguards:

- **Administrative Safeguards:** Rules and procedures, such as mandatory privacy training and internal policies.
- **Physical Safeguards:** Measures to protect physical assets, like using **locked file cabinets** and keeping records in **secure rooms** to prevent unauthorized intrusion.
- **Technical Safeguards:** Controls within computer systems to protect electronic data, such as strong **passwords, access controls,** and **encryption** (scrambling data so only authorized users can read it).

3. Privacy Breaches

A **Privacy Breach** is a security incident involving the **loss of, unauthorized access to, or unauthorized disclosure of personal information**. Breaches often result from human error or malicious activity.

Examples of Common Breaches:

- **Loss/Theft:** Losing an unencrypted work laptop or device.
- **Disclosure Error:** Sending an email containing PII to the wrong person.
- **Unauthorized Access:** An employee "snooping" on a patient or client record they are not authorized to view.

Mandatory Reporting (Real Risk of Significant Harm):

If a breach occurs and a reasonable person would conclude there is a **Real Risk of Significant Harm (RROSH)** to the individual, the organization must immediately report the incident to the affected person and regulatory bodies. **Significant Harm** is defined as serious damage or injury, such as **identity theft, financial loss, humiliation, or damage to employment**.