

# 5 Core Types of Sensitive Information



## PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII refers to any data that can trace an individual's identity. This type of information is vulnerable to misuse and requires robust protection.

- **Personal Details:** Full name, home address, email, phone number, and even personal photos.
- **Identification Numbers:** Unique IDs like Social Security, passport, driver's license, and patient IDs.
- **Digital Identities:** Online identifiers such as usernames, account numbers, IP addresses, and mobile device IDs.
- **Biometric Records:** Fingerprints, retina scans, or other unique physical identifiers.
- **Personal Characteristics or Preferences:** Physical traits (height, weight) and personal habits (shopping or browsing history).



## FINANCIAL INFORMATION

This category includes details related to personal or business financial accounts. Exposure of financial data can lead to fraud or theft.

- **Banking Information:** Account numbers, routing numbers, and bank details.
- **Credit and Debit Card Info:** Transaction details, card numbers, and receipts.
- **Income and Tax Info:** Income sources, tax returns, and social security benefits.
- **Investment Info:** Stocks, bonds, retirement accounts, and securities.
- **Transaction Info:** Online identifiers tied to financial activities.



## PROTECTED HEALTH INFORMATION (PHI)

Health data covers information about an individual's physical and mental well-being. It's highly sensitive and must be safeguarded.

- **Medical History:** Past conditions, surgeries, allergies, and medications.
- **Diagnostic Info:** Lab results, test reports, and medical imaging.
- **Treatment Records:** Prescribed treatments, consultations, and therapy records.
- **Health Insurance Info:** Policy numbers, claims, and insurance-related data.
- **Family Health History:** Genetic data and familial health risks.
- **Lifestyle Information:** Habits like smoking, alcohol use, exercise, and diet.



## BUSINESS-SENSITIVE INFORMATION

This includes confidential business data crucial for a company's competitive advantage. Unauthorized exposure can harm business operations and reputation.

- **Trade Secrets:** Proprietary processes, formulas, or designs.
- **Client Information:** Contact details, financial data, and preferences.
- **Employee Information:** Personal, financial, and health data of employees.
- **Strategic Plans and Research:** New products, market strategies, and research.
- **Legal Documents:** Contracts, negotiations, and legal agreements.
- **Financial Records:** Profit-loss statements, balance sheets, and audit reports.



## HIGH-RISK DATA

This data, if exposed, can lead to severe consequences like identity theft, financial fraud, or national security risks. It requires the highest protection.

- **National Identification Numbers:** Social Security numbers and government-issued IDs.
- **Biometric Data:** Fingerprints, DNA, and other unique biological identifiers.
- **Legal Information:** Court records, criminal records, and legal proceedings.
- **Sensitive Government Info:** Data related to national security, military, and intelligence.
- **Sensitive Corporate Info:** Trade secrets, unpublished financials, and proprietary research.