Protecting Sensitive Information

Laws, regulations, industry standards, and internal corporate policies govern what information is sensitive and how it must be protected. Below are some critical types of sensitive information. Your company may well have other types of sensitive information, so review your corporate policies.

**Sensitive Personally Identifiable Information (PII)**

PII is information that uniquely identifies a person. If it can cause harm when exposed, it’s sensitive PII. Some PII like a national identification number (e.g. Social Security) or biometric identifier (e.g. fingerprint) is always sensitive PII. Other information is sensitive PII when combined with a person's name, or other unique identifier (e.g. phone number or address). Examples include:

- Driver's/driving license number
- Passport number
- Full credit card number
- Financial account numbers
- Birth date and birth place
- Citizen or immigration status

**Protected Health Information (PHI)**

Protected Health Information (PHI) is individually identifiable health information that is stored or transmitted. PHI includes any past, present, or future information about:

- Health status
- Medical diagnoses
- Health care provided
- Payment for medical services

**Confidential Information**

Confidential information is sensitive corporate information that, if exposed, can damage a company, either directly (e.g. attack or financial loss) or indirectly (e.g. loss of reputation or criminal charges.) Protect the following:

- Business information (e.g. trade secrets, contracts, acquisitions)
- Financial records, contracts, credit cards
- Marketing and sales (e.g. strategies, customer lists, plans, pricing)
- Operational data (e.g. physical plant details, network architecture)
- Technical information (e.g. specifications, documentation, source code, prototypes)
- Reports (e.g. internal, research and analyst)