Using Coro to protect against data loss and misuse

Organizations typically have regulatory, contractual, or ethical obligations to protect the data they hold about individuals.

To ensure the security and privacy of sensitive information, organizations must be able to demonstrate they have robust data protection measures in place. This includes the ability to ***manage access*** to sensitive information, to ***monitor*** data sharing and sending, and to ***store data securely***.

What counts as sensitive information

Sensitive information refers to data that is confidential, private, or otherwise protected by law, policy, or contractual obligation, and requires special care in handling, storage, and access.

Sensitive information typically falls under one of the following types:

- **Personally Identifiable Information (PII)**: Information that allows a reasonable inference of the identity of a person either directly or indirectly, such as full name, email address, passport number, or social security number. PII is covered by data protection regulations such as GDPR in Europe and state privacy law in the United States (for example, CCPA, NYPA, CPA).
- **Payment Card Industry (PCI)**: a set of security standards created by major credit card providers designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
- **Protected Health Information (PHI)**: Information about an individual's health or medical history that is collected, stored, used, or disclosed in the course of providing health care services, such as patient name, medical history, and health insurance details. PHI is protected by law under legislation such as the Health Insurance Portability and Accountability Act (HIPAA).
- **Non-Public Personal Information (NPI)**: personal financial information that is collected and stored by financial institutions, such as social security number, financial account numbers, home address, email address, income details, and employment information. NPI s protected by law under legislation such as the Gramm-Leach-Bliley Act (GLBA).

To see the list of data descriptors that Coro is able to identify as sensitive information, see **Data descriptors recognized by Coro**.

> **Important**
>
> Coro recognises sensitive data for defined descriptors in US-format only.

To learn more about the standards enforced for protecting sensitive information, see **Compliance**.