Data descriptors recognized by Coro Cybersecurity

Coro Cybersecurity can identify stored sensitive information on your user's devices that might be covered by regulatory or data compliance standards. Such information falls into one of the following categories:

- **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.
- **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.
- **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.

To learn more about how you can use Coro Cybersecurity to reduce the risk of data breaches and to protect sensitive information from unauthorized access and misuse, see **Using Coro Cybersecurity to protect against data loss and misuse**.

To learn more about the regulatory standards that apply to sensitive information, see **Compliance**.

The following table lists sensitive information detectors that Coro is able to identify:

Note

This table is subject to continuous review as Coro adds further detectors and categories over time.

Important

Coro recognises data for these descriptors in US-format only.

Detector Name	Type	Data Type I	Data Type II
Account Number	Content	NPI	
Annual Credit Report	Form	NPI	