Configuring monitoring settings

Strong data monitoring and detection controls are necessary to prevent sensitive information from being shared with, or accessed by, unauthorized users. One way to achieve this is by detecting sensitive information through the use of technologies for data governance.

Coro's data governance capability monitors in real-time and scans all outgoing communications for sensitive information, flagging to the administrator any instances where such information is sent to an unauthorized user or group of users.

Coro recommends monitoring the information types critical to your business or industry to achieve optimal results. For example:

- A company providing accounting services might collect personal customer information to effectively deliver its services. In this case, Coro recommends monitoring for **PII** and **PCI**.
- A company providing nursing services to patients would need to collect personal and health information as part of the service. Coro recommends monitoring for **PHI**, **PII**, and **PCI**.
- Automotive agency that provides loan services collects personal and financial information. Coro recommends monitoring **NPI** as the agency must comply with GLBA regulations.

> **Note**
>
> When a new workspace is created, all **User Data Governance** options are disabled by default. Permission settings only take effect after monitoring is enabled for one or more **User Data Governance** options.

To configure data monitoring:

1. **Log into the Coro console** and select **Control Panel** from the toolbar.

2. Select **User Data Governance**.
3. Select the **Monitoring** tab: