Introducing User Data Governance

Coro's **User Data Governance** aims to establish an all-encompassing and proactive strategy for correct and secure data handling by a business's end users (employees, contractors, third-party vendors, etc.), as well as risk mitigation for data breaches, data leaks, data loss, and other security threats when accessing, viewing, sharing, and moving data across the business's cloud apps and via email. Compliance with these strategies requires the definition and implementation of policies, procedures, and controls in accordance with applicable laws, regulations, and industry standards.

Coro's **User Data Governance** helps in meeting regulatory requirements. The following are some examples of regulatory requirements that Coro can assist you with:

- HIPAA
- GLB
- GDPR
- SOC2
- SOX

Coro's **User Data Governance** monitors for:

- PII (personally identifiable information)
- PHI (protected health information)
- PCI (payment card information)
- NPI (non-public information)

Additionally, Admin users can configure monitoring for the following business-sensitive data:

- Passwords
- Certificates
- Source code
- Data objects with specific keywords
- Specific file types