Ticket types for User Data Governance

To learn more about how Coro protects an organization's user data, see **Introducing User Data Governance**. To learn more about what information constitutes these sensitive data types, see **Regulatory sensitive information types**.

Coro generates tickets relating to data governance when it identifies security incidents involving the following sensitive data types:

- **NPI (Non-public information)**
- **PII (Personally identifiable information)**
- **PHI (Protected health information)**
- **PCI (Payment card information)**
- **Suspicious exposure of certificate**
- **Suspicious exposure of critical data**
- **Suspicious exposure of file type**
- **Suspicious exposure of password**
- **Suspicious exposure of source code**

> **Note**
>
> For an admin user to view sensitive data in the email content and findings sections of tickets related to **User Data Governance**, content inspection must be enabled. When disabled, these sections display a message stating *Access to sensitive data is restricted* if they contain sensitive data. For more information, see **Managing admin users**.

NPI, PII, PHI, and PCI

Coro detected that a user shared or emailed information that includes NPI, PII, PHI, or PCI, and the Admin user has **monitoring enabled** for that category. The Admin user might also have configured **permissions policies** governing user rights to access, or access and expose, these data types.

These tickets might require the attention of data compliance officers, in line with regulations such as GDPR, HIPAA, SOC2, and others, therefore are classified as *suggested for review* and automatically closed after the review period of two weeks.

Privacy sensitive data tickets include the following available actions: