

# Ticket types for Endpoint Data Governance

To learn more about how Coro protects an organization's endpoint data, see [Introducing Endpoint Data Governance](#). To learn more about what information constitutes these sensitive data types, see [Regulatory sensitive information types](#).

Coro generates tickets relating to endpoint data governance when incidents are identified that involve the following sensitive data types and the Admin user has enabled **Privacy sensitive data** settings in **Control Panel > Endpoint Data Governance**:

- **Endpoint drive with NPI**
- **Endpoint drive with PCI**
- **Endpoint drive with PHI**
- **Endpoint drive with PII**

## Endpoint drive with NPI

Coro detected unauthorized exposure of NPI (Non-Public personal information) data on the device (see [Regulatory sensitive information types](#).) Tickets are classified as *suggested for review* and are automatically closed after the review period of two weeks.

Action	Outcomes
<b>Close ticket</b>	<p>Close this ticket as considered remediated and take no further action.</p> <p><b>Note:</b> When a device is removed from protection, all open tickets associated with the device are automatically closed.</p>
<b>Encrypt drive</b>	<p>Encrypts the hard drive of the device.</p> <p>A record is added to the Activity Log:</p> <p>"Drive encryption was requested on &lt;device name&gt; of user &lt;user&gt; (drive: '&lt;drive &gt;')"</p> <p>When drive encryption is complete, a record is added to the Activity Log:</p> <p>"Drive was encrypted on &lt;device name&gt; by &lt;user&gt;"</p> <p>Encryption keys are stored on both the device (by BitLocker) and on the Coro servers.</p>