Data Governance and Privacy Policy

Objective

The main objective of this data governance and privacy policy is to ensure the safe and responsible handling of sensitive data, such as personal health information and confidential business information. This includes protecting the privacy and security of individuals whose data is being collected and processed, as well as ensuring compliance with relevant laws and regulations.

Additionally, the data governance and privacy policy aims to:

- Define roles and responsibilities for data management, access, and use
- Ensure data accuracy, completeness and consistency
- Establish guidelines for data retention and deletion
- Manage data breaches and security incidents
- Regularly review and update the data governance and privacy policy to ensure it remains effective and relevant.

Overall, the objective of data governance and privacy policy for Indoco Remedies Limited (Indoco) is to maintain the trust and confidence of patients, customers, and other stakeholders by handling data in an ethical and responsible manner.

Scope

This policy is applicable to all associates, contractors, and third parties who have contractual obligations to abide by it and who have access to Indoco systems. This policy concentrates on the following areas,

- **Personal Health Information (PHI)**: The policy will govern the collection, storage, use, and disclosure of PHI, which includes any information that can be used to identify a patient and that relates to their past, present, or future physical or mental health.
- **Research Data**: The policy will also govern the collection, storage, use, and disclosure of data collected during clinical trials and research studies.
- Marketing and Sales Data: The policy will govern the collection, storage, use, and disclosure of data related to Indoco's marketing and sales activities, including customer information, sales data, and market research data.
- **Employee Data**: The policy will govern the collection, storage, use, and disclosure of employee data, including personal information, payroll data, and performance records.

- **Information Systems and Technology**: The policy will govern the security and privacy of Indoco's information systems and technology, including data encryption, firewalls, and intrusion detection systems.
- **Third-Party Data**: The policy will govern the collection, storage, use, and disclosure of data obtained from third-party sources, such as vendors and partners.

- **Incident Management**: The policy will include procedures for identifying, reporting, and responding to data breaches or other incidents that may compromise the privacy and security of personal data.

The scope of the data governance and privacy policy may also be extended to cover additional areas, as deemed necessary by Indoco.

Guiding Principles

Our data governance and privacy are governed by the following principles,

- **Compliance with laws and regulations:** Ensure compliance with all applicable laws and regulations related to data governance and privacy.
- **Data protection:** Implement robust security measures to protect sensitive data from unauthorized access, use, and disclosure.
- **Transparency and accountability:** Clearly communicate Indoco's data governance and privacy policies to all stakeholders and be accountable for ensuring compliance with these policies.
- **Data minimization:** Collect and process only the minimum amount of data necessary to achieve specific business goals.
- **Data accuracy:** Ensure that data is accurate, complete, and up-to-date.
- **Data retention:** Establish clear guidelines for how long data is retained and when it is deleted.
- **Privacy by design:** Incorporate privacy considerations into the design and development of products, systems, and processes.
- **Regular Audits and Risk Assessment:** Regularly assess data governance and privacy risks, and conduct audits to ensure compliance with policies and procedures.
- **Incident Management:** Have a clear process in place for managing and reporting data breaches or other incidents that may compromise the privacy and security of personal data.
- **Employee Training:** Regularly train employees on data governance and privacy policies and procedures, and ensure that they understand the importance of protecting sensitive data.