Responsible AI Policy

Version 1.0

Table of Contents

1. Purpose

Cipla's purpose of Caring for Life guides the responsible use of Artificial Intelligence (AI). Cipla is committed to ensuring that AI is developed, procured, deployed and used in a manner that is ethical, safe, secure, transparent, sustainable and compliant with applicable laws, regulations and internal policies.

This policy sets out Cipla's enterprise-level Responsible AI principles, governance expectations and sustainability commitments. It is intended to support patient safety, product quality, privacy, information security, regulatory compliance, stakeholder trust, and prioritize responsible innovation.

2. Scope and Applicability

This policy applies to all Cipla employees, contract staff, consultants, vendors, partners and third parties who design, develop, procure, deploy, integrate, operate or use AI systems on behalf of Cipla.

It applies to internally developed AI solutions, externally procured AI-enabled products, embedded AI capabilities within enterprise applications, cloud-hosted AI services, generative AI tools, predictive analytics, machine learning models, intelligent agents and AI-assisted business processes across Cipla's global operations.

Where stricter legal, regulatory, privacy, cybersecurity, quality, pharmacovigilance, contractual or market-specific requirements apply, those requirements shall take precedence.

For the purposes of this policy, an AI system means a machine-based system that is designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment, and that infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

This Policy is published for informational and transparency purposes. It reflects Cipla's principles and current practices and does not create, and shall not be construed as creating, any binding legal obligation, contractual right, warranty, or third-party beneficiary right. Nothing in this Policy constitutes legal, medical, clinical or professional advice.

3. Responsible AI Principles

Cipla shall adhere to the following principles:

- Human oversight and patient safety: AI shall augment human expertise and support human decision-making and shall not replace human accountability. Decisions impacting patients, product quality, regulatory compliance or healthcare outcomes shall remain subject to appropriate human oversight.
- Fairness and non-discrimination: AI systems shall be designed, tested and monitored to reduce unfair bias, unintended discrimination and inequitable outcomes, and promote inclusive development.
- Transparency and explainability: AI use shall be transparent to relevant stakeholders where appropriate. To the extent possible, material AI-generated outputs and AI-assisted

recommendations shall be explainable, traceable and sufficiently documented to support review and auditability.

- Privacy, confidentiality and data protection: AI systems shall be used in a manner that protects personal data, patient data, employee data, healthcare professional data, partner information, intellectual property and confidential business information through appropriate data governance, access control and privacy and security safeguards.
- Security and resilience by design: AI solutions shall incorporate cybersecurity and resilience controls to prevent unauthorized access, data leakage, adversarial misuse, prompt injection, manipulation or cyber compromise.
- Accountability, compliance and sustainability: Each material AI use case shall have an identified owner and be governed using a risk-based lifecycle approach. Environmental impact and efficient use of compute, cloud, storage and infrastructure shall be considered for significant AI deployments.

4. Responsible and Prohibited Use of AI

AI shall only be used for legitimate business, scientific, healthcare, manufacturing, quality, commercial, operational or corporate purposes consistent with applicable laws, ethical standards and Cipla policies. AI systems shall not compromise patient safety, human dignity, privacy, confidentiality, regulatory compliance, business integrity or information security.

The following AI uses are prohibited:

- Social scoring of individuals or groups.
- AI systems that are designed to manipulate human behaviour in a deceptive, coercive, exploitative or harmful manner.
- Exploitation of vulnerabilities arising from age, disability, health condition, financial status, socio-economic circumstances or other personal vulnerabilities.

The following AI uses are restricted and require documented risk assessment and approval through Cipla's AI Governance Framework, and are permitted only where lawful in the relevant jurisdiction:

- Biometric identification, biometric surveillance, facial recognition, behavioural monitoring or similar surveillance activities.
- Fully autonomous decisions in critical healthcare, quality, regulatory, employment or high-impact business contexts without appropriate human oversight.
- Any AI application that may create unacceptable risk to patient safety, product quality, privacy, confidentiality, cyber resilience or regulatory compliance.
- AI used in recruitment, employment related decisions or worker management shall be treated as a high-risk use case and shall be subject to bias evaluation and appropriate notice to affected candidates or workers

High-risk or sensitive AI use cases shall be subject to enhanced risk assessment, documented justification, approval, monitoring and periodic reassessment before and after deployment.

5. Data Governance, Privacy and Security

AI solutions shall endeavour to use data that is lawfully obtained, relevant, accurate, appropriate, traceable and governed in accordance with Cipla's Data Governance, Information Security, Privacy, Quality Management and Records Management requirements.

Where AI systems process personal data, Cipla shall comply with applicable data protection laws, including the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 in India and the General Data Protection Regulation in the European Union. Data protection impact assessments and due diligence to verify that algorithmic software does not pose a risk to the rights of data principals shall be undertaken where required, including where Cipla maybe designated a Significant Data Fiduciary.

Data used for AI training, testing, validation, inference, monitoring or reporting shall be assessed for suitability based on intended purpose, data sensitivity, regulatory impact and stakeholder risk.

Use of non-approved public AI tools or public data sources for confidential, regulated, proprietary or sensitive Cipla information is prohibited unless reviewed and approved through the designated governance process.

AI systems shall be protected through appropriate safeguards including access management, data minimization, purpose limitation, secure configuration, logging, monitoring, incident response and cybersecurity controls proportionate to risk.

6. Transparency, Human Review and Accountability

Where required by applicable law, Cipla shall disclose when individuals are interacting with an AI system and shall mark or label AI generated content, including synthetic audio, image, video and text, in the manner the law prescribes. Beyond legal requirements, material AI-generated content, recommendations, analysis, outputs or decision-support results shall be identified as AI-assisted or AI-generated where appropriate and technically feasible.

Individuals interacting with AI-enabled systems should be informed where AI materially influences communications, recommendations or decisions affecting them.

Affected stakeholders shall have access to appropriate channels for clarification, escalation and human review for significant AI-influenced outcomes, subject to applicable law, contract, process design and business context.

Final accountability for business decisions shall remain with designated human decision-makers. AI outputs shall not substitute professional judgement, clinical judgement, quality review, regulatory accountability or management accountability in critical contexts.

Cipla retains all intellectual property rights in AI-assisted outputs involving material human authorship or direction generated in the course of its business, including research and development outputs, to the extent recognized under applicable law.

AI-related content, tools, chatbots or decision-support features made available on Cipla's public channels, if any, are provided for informational purposes only and do not constitute, and are not a substitute for professional medical advice, diagnosis or treatment.

7. Sustainability and Environmental Responsibility

Cipla recognizes that significant AI deployments may have environmental impact through model development, high-volume inference, data centre capacity, cloud consumption, storage and compute-intensive workloads.

Environmental considerations shall be integrated into evaluation, design, procurement, deployment and operation of significant AI technologies where material and reasonably practical.

Cipla shall promote efficient use of compute resources, cloud infrastructure, storage and model architectures; encourage model reuse and workload optimization; and collaborate with technology partners that demonstrate responsible environmental practices.

Where feasible and material, Cipla shall track the contribution of significant AI initiatives to sustainability outcomes such as energy efficiency, emissions reduction, waste reduction, resource optimization, productivity improvement and process efficiency.

8. Governance, Oversight and Program Commitments

Cipla shall maintain an enterprise Responsible AI Governance Framework led through appropriate cross-functional representation from Data & Digital, Enterprise Architecture, Information Security, Privacy, Legal, Quality, Risk, Compliance, Human Resources, Procurement, Sustainability and relevant Business Functions.

The framework shall support risk-based assessment and approval of AI use cases, defined ownership and accountability, AI use case inventory and classification, lifecycle documentation, human oversight, monitoring, issue escalation, incident reporting and continuous improvement.

Role-appropriate Responsible AI awareness and training shall be provided to employees, AI users, developers, owners and approvers based on their responsibilities and risk exposure.

Cipla shall monitor emerging AI laws, regulations, standards and stakeholder expectations, and evaluate alignment with recognized AI management standards such as ISO/IEC 42001, the NIST AI Risk Management Framework and the India AI Governance Guidelines issued by the Ministry of Electronics and Information Technology as part of its maturity roadmap.

Minimum program commitments for sustainability and responsible AI alignment

Commitment	Policy expectation
AI inventory and risk classification	Cipla shall aim to maintain human oversight of material AI use cases based on intended use, impact and risk.

Human oversight	Cipla shall require qualified human review for significant AI-assisted decisions and high-risk use cases.
Fairness, drift and performance	Cipla shall aim to monitor material AI systems for accuracy, reliability, fairness, security, model drift and unintended impacts.
AI-generated content disclosure	Cipla shall label or disclose AI-generated or AI-assisted outputs where appropriate and technically feasible.
Sensitive capability controls	Cipla shall restrict sensitive AI capabilities to approved use cases and authorized users vide its internal AI Governance Policy.
Sustainability metrics	Cipla shall aim to consider and track, where material- compute efficiency, cloud consumption, model reuse and sustainability business outcomes.
Training and awareness	Cipla shall provide role-appropriate training on ethical, secure, compliant and responsible AI use to the intended stakeholders from time to time.
Incident reporting	Cipla shall set up appropriate internal escalation matrix to report and address AI-related incidents, policy violations, model failures, data leakage, bias concerns or unintended impacts.

9. Third-Party AI Solutions and Supplier Controls

Third-party AI-enabled products, platforms, services and embedded AI capabilities shall be reviewed using a risk-based approach before procurement, integration, deployment or production use.

Reviews shall consider data processing, cybersecurity, privacy, intellectual property, model transparency, auditability, contractual obligations, data residency, restrictions on training vendor models using Cipla data, incident notification obligations, regulatory support, continuity, exit requirements and environmental responsibility practices where material.

Suppliers and technology partners may be required to provide appropriate evidence of security, privacy, responsible AI commitments, model limitations, assurance reports, incident management and environmental responsibility practices.

10. AI Incident Reporting and Corrective Action-

Potential, suspected or actual AI-related incidents, policy violations, unintended impacts, bias concerns, data leakage, security events, privacy events, model failures or inappropriate AI use shall be

reported through appropriate Cipla incident, risk, compliance, privacy or information security channels.

Corrective actions shall be defined based on severity, impact, affected stakeholders, regulatory implications and business risk. Actions may include additional controls, model retraining, output restrictions, user communication, suspension, retirement, supplier action or formal incident response.

11. Policy Review and Maintenance

Cipla reserves the right to modify this Policy from time to time without prior notice. The updated version will be posted on this website with a revised effective date.

Contact information

If you have any questions, concerns, or requests regarding this Policy, you may contact us at:

Cipla Limited

Cipla House, Peninsula Business Park,

Ganpatrao Kadam Marg, Lower Parel,

Mumbai - 400013, India

Email: globalprivacy@cipla.com

Last updated: September 2nd, 2026