GALDERMA

EST. 1981

Last updated July 2026

Information Security & Artificial Intelligence at Galderma

At Galderma, we believe that Artificial Intelligence ("**AI**") can support our mission of advancing dermatology for every skin story. As such, we already selectively leverage AI across the full product lifecycle, from research and development to manufacturing, distribution and customer engagement. With AI, Galderma seeks to improve efficiency, and enhance decision-making to better serve patients, consumers and customers worldwide.

When deploying AI across the organization, Galderma is committed to always ensuring secure, compliant, ethical and responsible use, aligned with Galderma's Integrated Dermatology Strategy. To uphold this commitment, Galderma built on existing Information Security processes and procedures to develop a tailored AI Foundation Framework ("**Framework**"). The Framework lays the groundwork for a comprehensive approach to AI at Galderma, providing a structured approach to governance, risk management and the deployment of AI solutions. It is designed to ensure alignment with Galderma's strategic objectives while addressing potential risks and safeguarding compliance with regulatory and ethical standards. The Framework includes six key principles for the responsible and ethical use of AI, an AI governance model structured around two core pillars and a dedicated responsible use of corporate AI tools policy.

Six Key Principles for the Responsible Use of AI

AI usage and the deployment of AI solutions[1] at Galderma is built on six key principles.

Developing and Using AI responsibly

In addition to complying with all applicable laws, regulations, external guidelines (e.g., GDPR, HIPAA, GxP) and internal policies, AI solutions should promote fairness by preventing bias and discrimination. Further, human decision-makers should always remain accountable and responsible for decisions supported or informed by AI solutions.

Testing AI solutions with use cases

AI solutions should be systematically evaluated through defined AI use case assessments before deployment to ensure they deliver business value while managing risks appropriately. Evaluation criteria include risk levels (i.e., data, use case and operational risks), business value, feasibility and compliance.

Maintaining Data Governance and Security

[1] Note that, for the purpose of this document, an AI solution refers to any application, system, model or capability that uses AI to generate outputs across the organization, including but not limited to recommendations, business processes assistance or decision support.

To protect sensitive information and guarantee the reliability of AI solutions, strong data governance and security should be enforced. This includes only using approved and trusted data sources and relying on encrypted data (possibly anonymized) that must be stored securely according to compliance regulations. Further, access to AI solutions and datasets must follow Role-Based Access Control (RBAC) principles.

Managing AI Risk and Compliance

All risks associated with AI solutions should be proactively identified, assessed and managed throughout solutions' lifecycles to ensure they remain safe, reliable and compliant before, during and after deployment. A structured risk assessment framework, aligned with industry regulations and internal risk policies, should be used with high-risk use cases (e.g., legal automation, hiring models) requiring additional approvals and controls.

Monitoring and Continuously Improving AI Solutions

Compliance, accuracy and efficiency of AI solutions should be continuously monitored throughout their lifecycle. This ensures that AI solutions remain accurate, secure, compliant and aligned with evolving risks, regulations and business needs. Further, regular reviews support the early identification of issues such as performance drift or security vulnerabilities and drive the ongoing improvement of AI solutions and governance practices.

Promoting Transparent and Explainable AI

AI decisions should be understandable and interpretable. When appropriate, AI solutions must provide sufficient information on how outputs are generated and how these solutions support informed decision-making, including through incorporating explainability tools (e.g., SHAP, LIME).

Galderma AI Governance Model

The Galderma AI Governance Model establishes governance structures, including decision-making and oversight mechanisms, to ensure that AI technologies are developed, evaluated, deployed and managed in line with the six key principles of the responsible use of AI and in a structured, efficient and risk-informed manner.

While the Galderma AI Governance Model is structured around two core pillars detailed below, the AI Governance Committee serves as the organization's primary decision-making body for all AI-related topics. Mandate of the AI Governance Committee includes providing strategic oversight, reviewing key AI initiatives, and ensuring AI investments, risks and priorities are managed consistently across Galderma. It is chaired by Galderma's Global Head of IT and composed of all relevant representatives across key functions, including Finance, Legal or Procurement.

AI Use Case Management Process

Galderma follows a standardized process for categorizing, evaluating and approving AI use cases across the organization.

Categorization of use cases is made according to a comprehensive catalogue of six AI application types, clear descriptions and specific examples. Some specific use cases are prohibited by default, without going through the evaluation and approval steps. Evaluation of use cases is based on four dimensions:

- Business value: How is the AI solution contributing to Galderma's organizational objectives?
- Feasibility: How feasible is it to deploy the AI solution across Galderma?
- Data readiness: Does Galderma data match the AI solution (incl. relevance, quality, compliance, accessibility and security)?

- Impact and scalability: How scalable is the AI solution?

Each dimension is broken down into specific scoring criteria with a weight assigned. By combining scores and applying weights, each use case is assigned a specific grade and a status (i.e., “Go”, “Validate/go”, “No-go”). If a use case is granted a “Go” status, it goes through detailed risk assessment. Validation is based on the outcome of the risk assessment for “Go” use cases. A use case receiving a “Validate/go” status require further validations/analysis before potentially being assigned a “Go” status while “No-go” use cases are dropped.

Data Governance Framework

Galderma integrates AI solutions into a robust data governance framework aligned with ISO/IEC 42001:2023. The data governance framework relies on structured data sensitivity classification & controls, data readiness assessments and tailored data privacy and security measures.

Data sensitivity classification & control guarantees that all data feeding AI solutions are adequately secured (incl. encrypted and strictly controlled when required) depending on their sensitivity and that they are integrated into appropriate and authorized repositories to comply with all relevant data protection laws (e.g., GDPR, CCPA). Further, before using any dataset for AI solutions, it needs to pass through a detailed data readiness assessment checklist to review the relevance, quality, compliance accessibility and security of the data. Finally, data security measures are enforced. These include access control (i.e., Role-Based Access Control, Multi-Factor Authentication, User Activity Logging), data protection (e.g., encryption, secure storage environments), system integrity (e.g., regular penetration testing, incident response testing, vulnerability management) and threat detection. By relying on trusted data sources and appropriated technical safeguards, Galderma supports secure AI solutions deployment while minimizing operational, cybersecurity and privacy risks. Note that third-party AI solutions may only be used after completion of Galderma’s applicable risk assessments and approval processes. Appropriate contractual, technical and organizational safeguards must be established before solution authorization or deployment.

Responsible Use of Corporate AI Tools Policy

Galderma enforces the responsible and ethical use of AI across the organization through a specific group-wide policy.

This policy defines clear guidelines aligned with the Six Key Principles for the Responsible Use of AI that all employees, customers, suppliers, contractors and any other person who has access to the AI solutions provided by Galderma must follow. It defines user responsibilities, usage guidelines, integration of third-party AI solutions and required behaviors to ensure AI is used securely, ethically and in compliance with company policies and applicable regulations. The policy reinforces that users may only use AI solutions approved by Galderma through the applicable governance, security and compliance review processes and that confidential, proprietary, personal or regulated information must not be entered into non-approved AI solutions. The policy also outlines best practices for protecting sensitive information, maintaining human accountability, and preventing the misuse of AI solutions while enabling employees to use these safely and effectively in their daily activities. Galderma employees are regularly trained on that policy.