The EU AI Act & Pharma: Compliance Guide + Flowchart
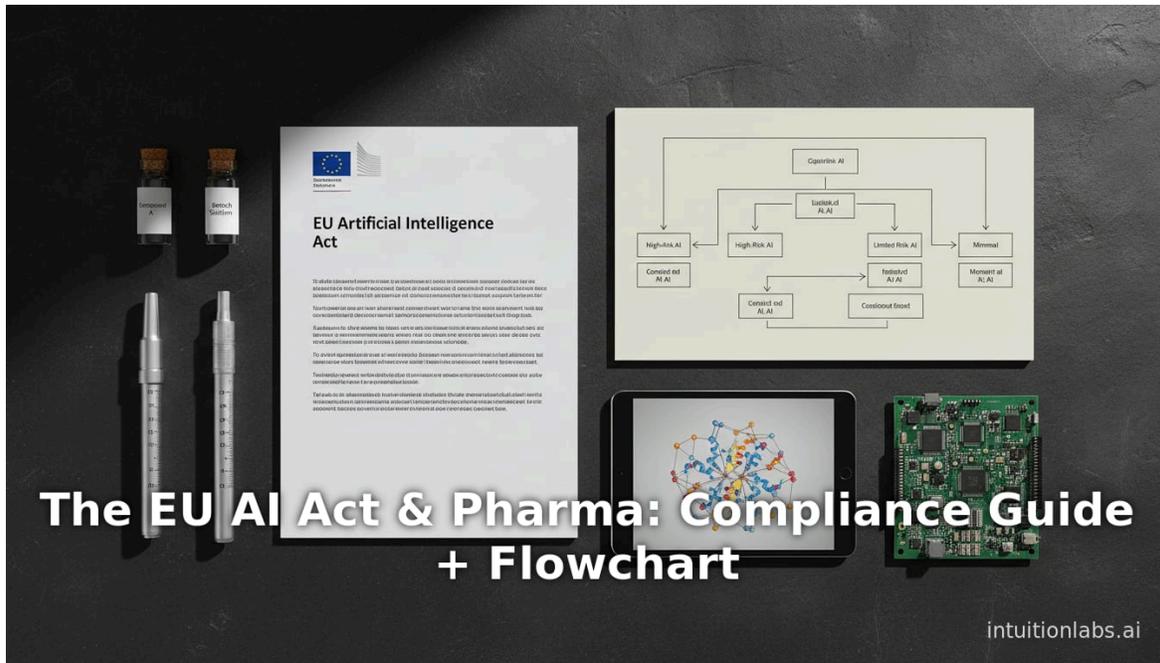
By InuitionLabs.ai • 10/18/2025 • 35 min read

eu ai act   pharmaceutical regulation   ai in pharma   high-risk ai   compliance   sop

medical device regulation   gxp

Executive Summary

The EU **Artificial Intelligence (AI) Act** – poised to become the world's first comprehensive AI law – will profoundly affect pharmaceutical companies that develop, use, or procure AI systems. Enacted in August 2024, the Act adopts a risk-based approach, categorizing AI into *unacceptable*, *high-risk*, *limited-risk*, and *minimal-risk* applications (www.pharmtech.com) (www.pharma-iq.com). Unacceptable uses (e.g. illegal social scoring) are banned, while high-risk uses (including many life-science applications) face stringent requirements for transparency, data governance, risk management, human oversight, and documentation (pharmaphorum.com) (www.europeanpharmaceuticalreview.com). Limited-risk applications (e.g. simple chatbots) must observe basic transparency or notice obligations, and minimal-risk uses face only voluntary guidelines (pharmaphorum.com) (www.pharmiweb.com).

For **pharmaceutical firms**, this framework adds a new compliance layer atop existing regulations (such as GMP, medical-device rules, and data privacy laws) (www.europeanpharmaceuticalreview.com) (www.orrick.com). In practice, virtually all AI systems used directly to support patient safety or treatment decisions (e.g. diagnostic algorithms, clinical decision support, patient monitoring apps) will be deemed high-risk (www.iqvia.com) (pharmaphorum.com). These systems must undergo formal conformity assessment, stringent risk management, and ongoing post-market monitoring. AI tools used in research-only contexts (e.g. early drug discovery models) are generally *exempt* from AI Act obligations (www.pharmtech.com) (www.orrick.com). Notably, the **European Federation of Pharmaceutical Industries and Associations (EFPIA)** has observed that "AI-enabled tools used in pharma R&D are exempt," whereas digital health and medical AI (even if low risk) are covered by the Act (www.pharmtech.com).

Compliance deadlines come in phases. Prohibited practices take effect on **2 February 2025**, obligations for general-purpose AI (such as large language models) on **2 August 2025**, and full high-risk and transparency requirements by **2 August 2026** (www.pharmtech.com) (securiti.ai). These obligations – including hefty fines (up to €35 M or 7% global turnover) for breaches (www.burges-salmon.com) (www.lachmanconsultants.com) – require pharma companies to act now. Key preparatory steps include: **inventorying all AI uses**, classifying each by risk, integrating AI compliance into quality systems (e.g. risk management under ICH Q9), establishing governance and documentation practices, and training staff on AI literacy (www.lachmanconsultants.com) (www.mastercontrol.com). A compliance *flowchart* should guide decision-making (see Figure 1). Likewise, a standardized set of **Standard Operating Procedures (SOPs)** should be drafted, covering areas like data governance, change control for AI models, performance monitoring, and incident reporting.

This report provides a comprehensive guide to EU AI Act compliance in the pharmaceutical sector. After an introduction and historical background, we analyze the Act's structure,

obligations, and implications for pharma R&D, manufacturing, clinical trials, medical devices, marketing, and data management. We include data (e.g. market trends, investment figures) and expert perspectives, and illustrate with industry examples (Novartis, Pfizer, BMS, Sanofi). Recommended compliance processes are detailed, including flowcharts and sample SOP outlines. The report concludes with a discussion of future directions (liability rules, global impacts, regulatory sandboxes) and a set of practical recommendations. All claims are backed by authoritative sources.

Introduction and Background

Evolution of AI Regulation

Artificial intelligence – especially **machine learning** and **generative AI (GenAI)** – has revolutionized drug discovery, clinical development, manufacturing, and patient care in recent years (www.mordorintelligence.com) (www.pharmiweb.com). Pharmaceutical R&D is increasingly data-driven: global AI/pharma investments exceeded $12 billion in 2023 (www.iqvia.com), and AI is credited with compressing development timelines and costs (the industry faces ~$2.6B outlay per new drug) (www.pharmiweb.com) (www.mordorintelligence.com). Leading companies (e.g. Novartis, Pfizer, BMS, Sanofi) have launched multibillion-dollar initiatives with AI startups and tech partners to apply advanced algorithms to molecular design, clinical trial optimization, and personalized medicine (www.mordorintelligence.com) (www.cognizant.com).

These strides come with new risks and uncertainties. Late-stage trial failures, model biases, data quality gaps, and opaque "black box" algorithms have exposed critical vulnerabilities in AI use (www.cognizant.com) </current_article_content>(www.mastercontrol.com). Recognizing this, regulators worldwide are racing to establish guardrails. In Europe, the **EU Artificial Intelligence Act** (AI Act) emerged as a cornerstone of digital policy. First proposed by the European Commission in 2021, it was negotiated and provisionally agreed by late 2023 (www.lachmanconsultants.com) (www.cognizant.com). Officially adopted in 2024, it entered into force on 1 August 2024 (www.pharmtech.com). The EU intends the AI Act to be "risk-based", harmonizing rules across Member States and potentially setting the global standard for AI oversight (www.consilium.europa.eu) (www.pharmtech.com).

European policymakers take AI governance seriously. The Council of the EU lauded the Act as "ground-breaking" in harmonizing AI rules on a risk-based principle (www.consilium.europa.eu). It follows earlier digital rulebooks like GDPR, where fundamental rights drove regulation. Notably, under the Act, harm-causing AI uses are banned; high-risk uses face rigorous controls; lower-risk uses have light-touch requirements (pharmaphorum.com) (www.pharma-iq.com). The legislation also incorporates provisions on **AI literacy** (training staff), partially in force by 2025 (insights.citeline.com), and establishes an EU AI Office and multi-national sandboxes to foster safe innovation (www.cognizant.com) (www.cognizant.com).

Impact on Pharmaceutical Sector

The pharma industry is uniquely affected. Drugs and medical devices are already among the most regulated products, and AI is now embedded in nearly every aspect of drug development. Examples include: AI algorithms that scan chemical libraries to propose new drug candidates; predictive models for patient recruitment and trial design; image-analysis software for diagnostics; robotic process automation in manufacturing; and even AI chatbots for medical information. Many of these are likely to fall under the AI Act's **high-risk** category (see below). The Act's new requirements will thus layer onto existing regimes like Good Manufacturing Practices (GMP), Medical Device Regulation (MDR), and data protection laws. The European Federation of Pharmaceutical Industries and Associations (EFPIA) has stressed that AI regulation "must be fit-for-purpose, risk-based, non-duplicative, globally aligned, and adequately tailored" (www.pharmtech.com).

For pharma, compliance starts with awareness. Only **9%** of life-sciences professionals report understanding AI-related regulations well (www.mastercontrol.com) – a gap given AI's potential to add **$100 billion** of value to healthcare (www.mastercontrol.com). As Leverage et al. note, firms must integrate AI risk management into their Quality Management Systems (QMS) and existing compliance programs (www.lachmanconsultants.com) (www.mastercontrol.com). The Act's requirements – on data quality, traceability, transparency, and human oversight – often mirror GMP and ISO 13485 provisions, easing some integration but also demanding new documentation and training (www.lachmanconsultants.com) (www.mastercontrol.com).

In summary, the introduction of the EU AI Act represents a pivotal moment for pharma. It promises safer, more trustworthy AI, but also imposes significant obligations. Companies must now systematically assess each AI use case, assign risk levels, and implement matching controls. The following sections will unpack these obligations in detail and provide tools (flowcharts, SOP outlines) to achieve compliance efficiently.

The EU AI Act: Structure and Key Provisions

Risk-Based Classification

The AI Act organizes AI systems into **four categories** by risk level (pharmaphorum.com) (www.pharma-iq.com):

- **Unacceptable Risk:** AI uses that contravene EU values or fundamental rights (e.g. subliminal manipulation, social credit scoring, mass biometric surveillance) are outright **prohibited** (pharmaphorum.com) (www.pharma-iq.com). No pharmaceutical application is expressly banned, but deployment of general-purpose AI (GPAI) for unethical profiling in healthcare could similarly be disallowed.

- **High Risk:** Systems deemed high-risk face the strictest rules (pharmaphorum.com) (www.iqvia.com). High-risk AI covers:

- AI used as a safety component in products covered by existing EU law (Annex II). In pharma, this primarily means **software as a medical device**: for example, diagnostic algorithms, patient monitoring apps, therapeutic decision support, or any AI integrated into medical devices (MD) or in vitro diagnostics (IVD) requiring third-party conformity assessment (www.iqvia.com) (www.orrick.com). Under the MDR/IVDR definitions, most AI used for diagnosing, treating, or monitoring patients (class IIa, IIb, III devices) is high-risk (www.iqvia.com) (www.orrick.com).

- Specific uses listed in Annex III. Relevant examples include biometric categorization (e.g. facial recognition for patient ID), eligibility determination for healthcare or insurance, and triage for emergency care (www.orrick.com) (www.iqvia.com). (Notably, an AI tool that assigns patients to treatment arms or predicts disease severity arguably falls into these health-related Annex III cases).

In short, **most clinical and medical AI systems in pharma are high-risk**. Analytical tools that influence patient outcomes or resource allocation will require full conformity assessment (www.iqvia.com) (pharmaphorum.com). Conversely, AI used for administrative or research tasks (e.g. drug discovery algorithms, non-clinical modeling) generally lies in a lower-risk bucket.

- **Limited Risk:** AI systems with moderate risk (Appendix B in Act) get lighter requirements such as mandatory transparency (e.g. chatbots and some biometric categorization) (pharmaphorum.com). For pharma, this could cover internal virtual assistants, marketing chatbots, or customer support bots. These must, for example, disclose to users that "you are interacting with an AI tool" (pharmaphorum.com), but do not require full third-party assessments.

- **Minimal/No Risk:** All other AI uses (e.g. internal document processing, supply-chain optimizations) face virtually no new regulatory obligations beyond voluntary standards. Even large language models (LLMs) like ChatGPT fall here as "general purpose AI" unless used in a high-risk context (www.iqvia.com) (pharmaphorum.com). The Act philosophically treats these applications as safe, encouraging innovation while mandating basic data/logging transparency under its horizontal provisions (www.pharmtech.com) (securiti.ai).

The classification logic can be summarized (see **Figure 1**). Organizations first determine whether their AI system triggers existing sector rules (like being medical device software) or falls into an Annex III use case. If so, it is *deemed* high-risk (www.iqvia.com). If not, they ask whether it complies with minimal transparency rules (if limited risk) or is out of scope (minimal risk).

Risk Category	Coverage	Pharma Examples	Key Obligations
Unacceptable	AI violating fundamental rights or EU values (pharmaphorum.com) (e.g. manipulation, social scoring)	None specific to pharma (unlikely to apply)	Prohibited outright (pharmaphorum.com)
High Risk	Software as Medical Devices/IVDs (MDR/IVDR), or Annex III uses	Diagnostic algorithms, AI in patient monitoring, trial recruitment (health	Full conformity assessment (Annex IV), risk management, validated datasets, transparency (Annex III/Articles 10-15)

Risk Category	Coverage	Pharma Examples	Key Obligations
	(www.iqvia.com) (pharmaphorum.com)	triage) (www.iqvia.com) (www.iqvia.com)	(www.europeanpharmaceuticalreview.com) (www.mastercontrol.com)
Limited Risk	Specified uses requiring transparency (pharmaphorum.com) (e.g. chatbots, biometric categorization)	Customer-facing chatbots, content generators, certain analytic tools	Disclose AI use (Article 52); adhere to transparency logging (Article 13) (pharmaphorum.com)
Minimal Risk	All other AI systems	Basic R&D models, administrative analytics	No mandatory AI Act requirements (but voluntary ethics standards encouraged) (www.orrick.com)

Table 1: EU AI Act risk categories, illustrative pharma use cases, and general obligations. (Sources: EU AI Act text and analyses (www.iqvia.com) (pharmaphorum.com).)

Key Obligations for High-Risk Systems

Pharma companies should assume that **any AI system used in clinical or manufacturing operations that affects health** will trigger **high-risk** compliance (www.iqvia.com) (www.europeanpharmaceuticalreview.com). The following summarizes core obligations (many of which must be documented in quality records):

- **Risk Management System (Article 9):** A systematic, continuous process to identify and mitigate risks from AI logic and data (www.mastercontrol.com). Companies must perform thorough risk assessments throughout the AI lifecycle, including identifying biases, privacy impacts, and failure modes (www.mastercontrol.com) (www.lachmanconsultants.com). For example, pharmaceutical firms should integrate AI risk evaluation into their QMS/ICH Q9 frameworks (www.lachmanconsultants.com). Procedures must be in place to handle incidents (e.g. model errors triggering patient harm) and to revert to manual controls if thresholds are exceeded (www.mastercontrol.com).

- **Data Governance and Quality (Article 10):** High-risk AI must be trained and tested on high-quality data. This means ensuring data sets are accurate, representative, and traceable (pharmaphorum.com) (www.mastercontrol.com). Electronic records must comply with 21 CFR Part 11 and EU Annex 11 standards for audit trails and integrity (www.mastercontrol.com). In practice, pharma must document data provenance (source, cleansing methods), control for biases (e.g. ensuring clinical trial data doesn't underrepresent subpopulations), and maintain immutable logs of AI inputs/outputs (pharmaphorum.com) (www.mastercontrol.com).

- **Technical Documentation (Article 11 & Annex IV):** A comprehensive technical file is required, akin to medical device documentation. This file must describe the system's purpose, architecture, data handling, validation results, risk management plan, human oversight measures, and instructions for use (www.pharmtech.com) (www.europeanpharmaceuticalreview.com). Crucially, pharma companies must **label** their AI systems with a unique identifier and provide instructions on intended use, limitations, and proper operation (www.mastercontrol.com) (www.europeanpharmaceuticalreview.com). All design choices, assumptions, and testing protocols must be recorded. Many of these details overlap with existing medical device technical documentation (e.g. MDR software files), but under the AI Act they must explicitly address AI-specific features (like model adaptivity, "self-learning" behaviors) (www.pharmtech.com) (www.orrick.com).

- **Transparency and Provision of Information (Articles 12-15):** High-risk AI users must keep logs to ensure questions or incidents can be traced (www.mastercontrol.com). Patients or healthcare professionals affected by AI decisions have a right to an explanation. For example, if an AI system recommends a treatment, companies should be able to explain the data and reasoning behind that output (www.cognizant.com). In clinical contexts, regulators expect "continuous monitoring" of AI model performance and periodic reporting of any serious malfunctions or biases (pharmaphorum.com) (www.cognizant.com). Moreover, instructions must clarify the required level of human oversight and the expertise needed to supervise the AI (pharmaphorum.com) (www.mastercontrol.com).

- **Human Oversight (Article 14):** Pharma AIs must be designed for a defined human role in the loop. For example, clinicians must be able to overrule AI diagnoses, and operators of a manufacturing AI must understand its outputs before acting (www.orrick.com) (www.mastercontrol.com). Standard operating procedures should specify who monitors the AI and how to intervene if errors or atypical outputs occur.

- **Accuracy, Robustness, and Security (Article 15):** High-risk AI must meet strict performance criteria. For medical AI, this entails rigorous validation against clinical gold standards (pharmaphorum.com). Models should be robust to noise and adversarial attacks, as judged by testing under varied conditions. Cybersecurity measures are required to protect AI systems from tampering (www.mastercontrol.com). Companies must maintain cybersecurity protocols commensurate with those for other critical software (e.g. encryption, access controls, as emphasized under GDPR and GMP).

- **Audit & Certification:** Many high-risk AI systems will require **conformity assessment**. If an AI is itself a medical device, this assessment will be done by a notified body as part of CE marking (www.orrick.com). Otherwise, for stand-alone high-risk AI (like a medical triage tool not yet covered by device legislation), the provider must arrange an independent evaluation (internal or external) demonstrating compliance with the Act's requirements (the national regulators will publish conformity procedures). All assessment results must be appended to the technical documentation.

Table 2 below summarizes these obligations and typical pharma controls. In all cases, companies should integrate AI Act processes into existing compliance channels (e.g. Lean QMS, GMP change control, design reviews). Quality units should explicitly include "AI model modification" in their change-control protocols and treat AI software defects as "non-conformances" requiring corrective action plans.

Obligation Category	Requirements & Examples in Pharma	Control Measures/Documentation
Risk Management (Art.9)	Continual risk analysis of AI impact on patients/products	Maintain risk register; include AI-specific risks (algorithmic bias, data drift) in QMS (www.mastercontrol.com) (www.lachmanconsultants.com); SOPs for incident response.
Data Governance (Art.10)	High-quality training/test data; GDPR-aligned processing (www.mastercontrol.com)	Data lineage records, Part 11 audit trails, data access policies; bias-mitigation methodology (e.g. diverse datasets) (www.mastercontrol.com) (www.mastercontrol.com).
Documentation (Art.11 & Annex IV)	Complete technical file covering design, use, validation (www.mastercontrol.com)	Documents within QMS: Intended Use, System Architecture, Validation Reports, Clinical Performance Data, User Manuals (www.mastercontrol.com).
Transparency (Art.13)	Logging of AI outputs; explanation of decisions for patients	System logs; version control; documentation of explanation processes; informed consent forms noting AI use.
Human Oversight (Art.14)	Clear human roles; overrides; training requirements	SOPs detailing personnel responsibilities; training records; human-in-loop controls.
Accuracy & Security (Art.15)	Performance standards; resilience; cybersecurity	Validation studies (sensitivity/specificity analyses); penetration tests; encryption, user auth systems.
Conformity Assessment	Third-party or internal review of high-risk AI	Notified body audit for MD software; or internal AI audit by QA; registrar approval. Documentation of assessment is kept on file.

Table 2: Key compliance obligations under the AI Act for high-risk AI and corresponding controls in pharmaceutical operations (Sources: EU AI Act Articles and expert guidance (www.mastercontrol.com) (www.mastercontrol.com)).

Prohibited Practices and Other Provisions

While no routine pharma use is completely banned, companies must avoid **unacceptable practices**. The AI Act forbids any AI that manipulates subject behavior or infringes on rights (e.g. predictive scoring to deny treatment, biometric ID of patients without consent) (pharmaphorum.com). Decision-makers should screen for these risks; any AI flagged "unacceptable" must not be deployed.

Additionally, **transparency obligations** apply to certain limited-risk tools. For instance, if a pharmaceutical sales representative uses AI-generated images or text, EU law will soon require clear disclosure that the content is AI-created (an upcoming measure akin to the digital services regulation) (pharmaphorum.com). Though outside the core AI Act, companies must stay alert to related obligations (e.g. Europe's "deepfake" labeling rules).

Finally, the Act contains special rules for **foundation models** (large pretrained LLMs). Providers of these "general-purpose" AI (e.g. OpenAI, Google) must register and meet systemic risk checks by 2027. Downstream users (like pharma using an LLM for internal purposes) will generally have only transparency duties under the general framework (www.pharmtech.com). Nevertheless, companies deploying LLMs should monitor guidance, as misuse (for research hallucinations or data privacy breaches) could trigger liability.

Implementation Timeline

The AI Act's provisions come into effect in stages (www.pharmtech.com) (securiti.ai):

- **1 Aug 2024:** Act enters into force.

- **2 Feb 2025:** Ban on prohibited AI practices (Article 5) becomes binding, and some obligations on AI literacy (training) also begin (www.pharmtech.com) (insights.citeline.com).

- **2 Aug 2025:** Obligations for General-Purpose AI systems (transparency, risk management, cybersecurity, etc. under Chapter III) apply. Many core requirements on foundation models also kick in by this date (www.pharmtech.com).

- **2 Aug 2026:** Obligations for *all high-risk AI systems* (including those covered by MDR/IVDR) take full effect, as do broader transparency and conformity-assessment obligations (www.pharmtech.com).

- **2 Aug 2027:** Final compliance deadline for lighter provisions and national authority setups (securiti.ai) (www.pharmtech.com).

Pharmaceutical firms must track this schedule carefully. For example, the font-line obligations (July 2024) mandate *member states to designate national competent authorities* and *the EU to set up an AI Office* (www.pharmtech.com). Companies should aim to have internal governance (AI risk committees, guidelines) in place by early 2025, while gearing up for full system audits and CE marking adjustments by mid-2026.

Compliance Workflow: Decision Flowchart

To operationalize the above, we propose a **compliance flowchart** (schematic below) that the lead AI project manager or regulatory officer can use to triage AI systems:

1. **Identify AI System:** Does the digital tool meet the EU's definition of AI (i.e. uses machine learning/analytics to influence outputs autonomously)? If *no*, the Act does not apply; maintain normal best practices. If *yes*, proceed.

2. **Check for Exemptions:** Is the AI system used solely for R&D and kept within non-clinical contexts? Many pharma R&D tools (e.g. early drug design) may be exempt from stringent rules (www.pharmtech.com) (www.orrick.com). If exempt, focus on voluntary principles (see SOP notes); otherwise, continue as below.

3. **Determine Risk Category:**

- **Banned?** If the AI falls under any of the prohibited categories (e.g. it uses biometric surveillance of patients without consent), it cannot proceed (pharmaphorum.com).

- **High-Risk?** Check if the AI is part of a regulated device/software (MDR/IVDR) or in an Annex III use case. If so, classify as *High Risk* (www.iqvia.com) (www.orrick.com).

- **Limited-Risk?** If not high-risk but triggers transparency obligations (e.g. generative content tools, certain biometric functions), mark as *Limited Risk*.

- **Minimal:** Otherwise, the system is minimal-risk.

4. **Apply Controls Accordingly:**

- **Unacceptable:** Redesign the approach or cancel the project.

- **High-Risk:** Initiate conformity assessment process: allocate responsibility (provider vs user), set up risk management plan (Art.9), data governance plan (Art.10), and technical documentation. Engage competent authorities if needed. Plan for CE marking changes if MD.

- **Limited-Risk:** Ensure transparency notices (e.g. disclaimers that "AI was used" in any output). Document AI README files explaining the use.

- **Minimal-Risk:** No new legal steps required, but adopt internal best practices (data ethics, model validation guidelines) to avoid future liability.

5. **Internal Approvals & Training:** Regardless of category, any AI deployment should go through a compliance review board (involving Legal, Regulatory, IT, Data Science). Employees working with AI must be trained on the Act's basics (insights.citeline.com) (www.mastercontrol.com).

6. **Documentation and Audit:** Maintain records of the above decisions, risk analyses, tests, and training. Update this assessment whenever the AI's intended use or algorithm is significantly changed (which under the Act may trigger a new conformity review) (www.mastercontrol.com).

Compliance flowchart for EU AI Act in pharma

Figure 1: Example compliance flowchart for determining EU AI Act obligations in pharmaceutical organizations (conceptual).

(Figure 1 is a schematic representation of decision steps; it aligns with the official AI Act flowcharts published by legal experts (www.burges-salmon.com) (www.burges-salmon.com).)

Standard Operating Procedures (SOP) Starter Kit

Pharmaceutical companies should translate the flowchart into actionable **SOPs**. The following outline describes key SOP modules; each should reference internal documents (e.g. quality manuals) and be customized for company structure.

1. **AI Inventory SOP:**

- **Objective:** Systematically identify all AI systems (existing and planned) in the company's scope.
- **Steps:** Maintain a register of AI systems, noting purpose, development status, data used, and deployer (R&D group, manufacturing, etc.). Review this register quarterly.
- **Responsibility:** Data Governance or Digital Strategy office, in coordination with IT and department heads.

2. **Risk Classification SOP:**

- **Objective:** Assign each AI system to an EU AI Act risk category.
- **Steps:** For each AI in the register, answer criteria per Table 1. Document the classification rationale. For borderline cases, consult legal/regulatory affairs.
- **Records:** Classification forms should be stored in the QMS. If classified as high-risk, automatically generate a project folder for compliance documentation.

3. **Quality & Data Governance SOP (Art.10):**

- **Objective:** Ensure training/validation data quality and traceability.
- **Actions:** Implement data management plans: unique identifiers for datasets, lineage tracking, provenance logs. Data used to train AI must be checked for accuracy and bias.
- **Controls:** Incorporate Part 11/GMP Annex 11 controls for electronic records, including access controls and audit trails (www.mastercontrol.com).
- **Outputs:** Data Quality Reports; data stewardship assignments; formal validation of data pipelines.

4. **Risk Management SOP (Art.9):**

- **Objective:** Institute continuous risk analysis for AIs.
- **Procedures:** Use ICH Q9 framework adapted for AI. At introduction of any high-risk AI, perform a preliminary hazard analysis. Update risk log whenever model outputs cause any deviation or if underlying data changes.
- **Documentation:** Risk assessment forms with likelihood and impact scores; classes of risk (e.g. patient safety, privacy); mitigation plans.
- **Review:** Monthly or every release, whichever sooner.

5. **Technical Documentation SOP (Art.11 & Annex IV):**

- **Objective:** Compile and maintain a technical file for each high-risk AI.
- **Contents:** Implementation of items in Table 2: system description, architecture, algorithms, intended use, risk assessments, validation and test results, cybersecurity measures, user instructions (with human oversight requirements), and incident logs.

- **Maintenance:** Document must be regularly updated, e.g. for each software release. All versions must be archived as per QMS.

6. **Change Control SOP:**

- **Objective:** Control modifications to AI systems.
- **Process:** Any change to model architecture, training data, or intended use triggers a change request. The request must be reviewed for its impact on risk classification. Significant changes for high-risk AI require re-assessment under the Act.
- **Verification:** Test results for new version, updated risk analysis, sign-off by compliance officer.

7. **Incident Reporting SOP:**

- **Objective:** Handle AI malfunctions and near-misses.
- **Actions:** Define metrics for "serious incidents" (e.g. patient harm, security breach, data corruption). All significant incidents with AI must be reported internally and to authorities (as per EU or national rules). Maintain logs for external audits.
- **Template:** Incident report form with timeline, impact assessment, root cause.

8. **Training and AI Literacy SOP:**

- **Objective:** Ensure personnel understand AI compliance requirements.
- **Content:** Mandatory training modules on basics of AI Act, data ethics, and company AI policies. Special sessions for AI developers on documentation and validation standards.
- **Records:** Certification of attendance; refresher courses at least annually.

9. **Vendor and Outsourcing SOP:**

- **Objective:** Manage third-party AI procurement.
- **Procurement clause:** Contracts for AI (software/services) must include clauses ensuring the vendor's compliance with EU AI Act.
- **Due Diligence:** Before adopting external AI tools, verify providers' compliance (e.g. that their AI models have conformity declarations).

10. **Monitoring and Audit SOP:**

- **Objective:** Periodically audit AI compliance and governance.
- **Procedure:** Internal audits at least annually, covering all SOPs above, current classifications, and documentation completeness. External audits may follow after introduction of complex AI.
- **Audit Trail:** Maintain checklist of regulatory points (e.g. GCNL-ready by Aug 2025, per [59+L40-L42]) and track readiness.

These SOPs form a **starter kit**. Firms should refine each to align with their size and structure. For instance, a small biotech might combine some steps (e.g. risk classification done by CTO) whereas a large pharma would have dedicated AI governance teams. The key is to *document* each step.

Pharma-Specific Considerations

While the general framework above applies to all industries, the pharmaceutical context raises special points:

- **Integration with Medical Device Regulation (MDR/IVDR):** If an AI application also qualifies as a medical device by EU law (e.g. a diagnostic app or AI-driven test kit), it already follows MDR conformity assessment. In practice, this means the AI Act's requirements must be folded into the MDR processes (www.orrick.com) (www.iqvia.com). For example, CE-marking a device will now include certification that the embedded AI meets AI Act criteria. Thus, medical-device quality engineers should update templates (e.g. Device Master Records) to incorporate AI Act checklists (risk analysis, human oversight plan, etc.) (www.orrick.com) (www.lachmanconsultants.com). Conversely, *non*-device AIs (e.g. an AI used for internal process monitoring) must get treated in parallel via the AI Act framework.

- **R&D Exemption Nuance:** The Act explicitly states that *AI tools used solely in research and development of medicinal products are exempt* (www.pharmtech.com). This means predictive models in early drug design (not directly making patient decisions) have no new obligations. However, this exemption is narrow: once an R&D tool is used in a clinical phase (e.g. selecting trial endpoints), it may lose the exemption. Companies should carefully designate when an AI moves from research to regulated development, and apply SOPs accordingly.

- **Clinical Trials:** AI is increasingly used in trials (from patient matching to virtual cohorts). The Act revitalizes obligations to ensure trial AI is high-quality. For example, **synthetic control arms** (simulated patient groups generated by AI) are likely high-risk due to their impact on safety and efficacy decisions (pharmaphorum.com). Sponsors should treat these algorithms like significant new decision tools: document them fully, validate against real data, and include human researchers in the loop (pharmaphorum.com) (www.cognizant.com). Informed consent forms may need to note AI involvement if patient data or decision-making is affected.

- **Manufacturing:** AI is used in process optimization and quality control in pharma manufacturing (e.g. anomaly detection on production lines). These uses typically fall outside "medical purpose," but nonetheless can affect product quality. Firms should consider them under high-risk if they are safety-critical (e.g. an AI that decides when a bioreactor batch is out-of-spec). At minimum, robust validation and oversight are needed, and these AIs should undergo internal verification similar to other process systems. Documenting these sterilization or stability-prediction models aligns with good manufacturing practice.

- **Marketing and Administration:** AI in marketing (personalized advertising, content creation) generally is low risk under the Act, but may still be subject to future labeling rules (e.g. the Spanish law requiring "AI-generated content" labels). Administrative chatbots and assistants (e.g. answering physician queries) should follow limited-risk rules: they must inform users of the AI nature and verify outputs. Companies can mitigate compliance work by differentiating tools: classify internal-only automation (no patient involvement) as minimal-risk and focus resources on patient-facing AI.

- **Cross-border and Exterritorial Effects:** Non-EU affiliates of a global pharma must comply if their AI systems are used in EU-regulated activities. The Act binds providers and users worldwide if the deployment affects the EU market (www.iqvia.com) (pharmaphorum.com). Accordingly, multinational companies should consider establishing an EU representative or local legal entity to liaise with EU authorities (pharmaphorum.com). Post-Brexit, UK-based AI still must obey EU rules for use in Europe; fortunately, UK regulators (MHRA) are aligning their approach (e.g. the "AI Airlock" sandbox (www.cognizant.com)).

Data and Market Analysis

Pharma's shift to AI is underscored by strong market trends. The global AI-in-pharma market was **$4.35 B** in 2025 and is projected to reach **$25.4 B** by 2030 (42.7% CAGR) (www.mordorintelligence.com). Investment drivers include reduced discovery timelines, improved predictive accuracy, and regulatory impetus (e.g., agencies opening **"AI sandboxes"** to de-risk innovation) (www.mordorintelligence.com) (www.mordorintelligence.com). Indeed, strategic alliances abound: Bristol-Myers Squibb's $674M tie-up with VantAI and Sanofi's collaboration with OpenAI signal that AI is now core to R&D pipelines (www.mordorintelligence.com).

However, adoption is uneven. Surveys indicate substantial uncertainties: **only 9%** of pharma professionals feel well-versed in AI regulations (www.mastercontrol.com). Smaller biotech firms often lead in agility, embedding compliance quickly, whereas larger legacy companies have more friction in evolving data governance (www.europeanpharmaceuticalreview.com). Manufacturers are concerned about the complexity of aligning AI Act requirements with GMP: for example, integrating "AI change control" into existing versioning processes still lacks standardized guidance (www.europeanpharmaceuticalreview.com) (www.europeanpharmaceuticalreview.com).

Stakeholders also note only partial harmonization with global regimes. While the EU Act is pioneering, analogous efforts are rising (e.g. the forthcoming US FDA AI guidance, individual EU country laws, and interoperability with GDPR). Pharma companies therefore must prepare not only for EU law but for a patchwork of AI rules worldwide (www.pharmiweb.com) (www.orrick.com).

Case Examples and Expert Views

Expert Perspectives: Industry analysts warn that vague definitions in the Act could burden innovation (www.pharmiweb.com) (www.lachmanconsultants.com). For instance, Altimetrik's Vikas Krishan notes the broad, evolving AI definition may force firms to rehearse compliance for many systems (e.g., predictive analytics in trials) that are likely "high risk" (www.pharmiweb.com). He, along with other commentators, emphasizes the need for harmonized global standards (EU vs. US vs. UK) to avoid fragmentation (www.pharmiweb.com). In contrast, others (e.g. IFPMA, EFPIA) view the Act as a "clear message" boosting trust in AI, urging firms to see compliance as an opportunity to strengthen data governance and patient safety (www.mastercontrol.com) (www.lachmanconsultants.com).

Industry Collaboration: Recognizing the compliance challenges, regulatory sandboxes have been established. The Act mandates each Member State set up at least one AI regulatory sandbox by 2026 (www.cognizant.com). Pharma companies can apply to these controlled environments (e.g. France's forthcoming CNIL/HAS guidelines) to test new AI tools under supervision (www.europeanpharmaceuticalreview.com). Larger companies (Sanofi, Roche, etc.) are already teaming with smaller biotechs to jointly pilot AI innovations, combining agility with resources (www.cognizant.com). For example, the US-based Novartis real-life AI implementations (drug target identification via deep learning) and Pfizer's use of AI in trial design have demonstrated that, when managed correctly, AI can slash development phases without compromising compliance (www.cognizant.com).

Case Scenarios:

- *Case 1: Digital Pathology AI.* A European hospital biotech develops software that uses deep learning to analyze biopsy images. This AI is regulated as a Class IIa device under the MDR, so under the AI Act it is high-risk. The company updates its CE marking process: it conducts an Annex IV conformity assessment specifically for the AI component, documenting model training data, validation accuracy, and post-market surveillance plan. A human pathologist always reviews AI outputs (Article 14), and logs of cases are kept for audit (Article 61 data logging). This conforms with EU rules on medical-device AI (www.iqvia.com) (www.orrick.com).

- *Case 2: AI in Drug Discovery.* A large pharma uses an in-house machine-learning tool to suggest novel molecules. Since this is purely R&D (no immediate patient use) and "scientific research" is exempt, the AI Act imposes no formal obligations (www.pharmtech.com). The firm nonetheless follows internal quality guidelines: it validates the model on known active compounds and documents the results under its QMS (anticipating future regulations like FDA's guidance on AI/ML in drug development (www.orrick.com)). It proactively trains chemists on data bias and holds an internal audit of the AI pipeline annually.

- *Case 3: Virtual Clinical Recruiter.* A CRO deploys an AI tool that screens electronic health records to match patients to oncology trials. This qualifies as high-risk annex III (healthcare eligibility decision). The CRO's SOP requires a conformity check: they review the model for privacy (GDPR compliance), validate it on retrospective data (Article 15 requirements), and log all recruitment decisions made in part by the AI. Patients are informed in consent forms that an algorithm aids selection (Article 52 transparency). By 2026, the system will be formally registered with EU regulators as a high-risk health AI tool.

These scenarios illustrate that while the AI Act does not alter core scientific and regulatory standards (safety, efficacy, data quality), it mandates **processual compliance steps**. Pharma entities must build internal processes to ensure these steps occur, not just assume "business as usual."

Implications and Future Directions

Enforcement and Liability

EU enforcement will involve national AI authorities and the new EU **AI Office**. Member States must designate regulators (likely aligned with existing device/machine safety bodies) to inspect compliance. The AI Office (set up in 2024) will coordinate cross-border issues and, specifically, oversee foundation model risks (www.pharmtech.com). Early enforcement is likely to focus on prohibited uses and transparency (since these phases come first) (securiti.ai).

Parallel to the Act is the **AI Liability Directive** (due 2025) and revised **Product Liability Directive (PLD)**. Together, they ease the burden on victims to prove harm from AI (www.cognizant.com) (www.cognizant.com). For pharma, this means that if an AI-driven product (say, a diagnostic program) injures someone, the producer faces strict liability enhancements (e.g. proving no defect is harder). In practical terms, companies must strengthen quality controls: they cannot rely on disclaimers to escape responsibility. Documentation and audit trails (as mandated by the AI Act) become crucial evidence of due diligence.

Strategic and Competitive Effects

While compliance imposes costs, many experts view it as a competitive edge in the long run. The Act explicitly encourages the EU to become a global AI leader by building trust (www.lachmanconsultants.com) (www.pharmtech.com). Early adopter companies can market their AI tools as "Act-compliant", signaling safety to patients and partners. Moreover, robust AI governance often aligns with better general data practices. For example, systematic bias checks not only satisfy Article 10 but also improve drug trial demographics.

However, concerns remain. Some stakeholders worry that the burden of dual regulation (AI Act + healthcare laws) could slow innovation (www.pharmiweb.com) (www.lachmanconsultants.com). For instance, small biotech firms note that complex compliance processes require specialized legal/tech expertise (www.europeanpharmaceuticalreview.com) (www.europeanpharmaceuticalreview.com). In response, the Commission's **AI Pact** initiative encourages voluntary adoption of a compliance mindset early, and the EU has provided support packages for AI R&D (www.pharmtech.com).

Global and Future Outlook

The EU AI Act sets a precedent. Other economies (US, UK, China) are developing their own AI regulations, and the AAct's approach informs these debates. Pharmaceutical multinationals will likely strive for "one-fits-all" compliance, leveraging EU standards as a model. Indeed, the Act's extraterritorial scope means that any AI system placed on the EU market – whether made in Bangalore or Boston – must meet its requirements (www.iqvia.com) (pharmaphorum.com).

Pharma companies should thus anticipate a future where **AI regulatory alignment** is expected. Initiatives like the International Coalition of Medicine Regulatory Authorities (ICMRA) or ISO/IEC standard-setting may incorporate AI Act principles. R&D teams should design studies with regulatory scrutiny in mind (e.g. adopting explainable AI methods from the outset).

Finally, innovation continues. Foundation models (e.g. open-domain LLMs) will catalyze new therapeutic approaches (e.g. protein design, medico-scientific text mining) (www.mordorintelligence.com). The EU requires providers of these to share safety testing data (Article 68), and pharma firms using foundation models must watch for those disclosures. Meanwhile, constant vigilance on emerging tech (quantum AI, neuro-interfaces) will be needed, as the Act foresees further adjustments by 2027.

Conclusion

The EU AI Act introduces transformative rules that will reshape how pharmaceutical companies manage AI. Achieving compliance demands thorough understanding, organization-wide governance, and proactive planning. This report has detailed the Act's core components, timeline, and the specific implications for pharma – from R&D and clinical trials to manufacturing and marketing. We have outlined practical steps: a compliance flowchart, tables linking obligations to Pharma use cases, and an SOP framework to operationalize the law.

Moving forward, pharma firms should act now: assess AI inventories, launch training programs, and consult experts on adapting SOPs. Combining legal compliance with robust ethics will not only avoid hefty fines (www.burges-salmon.com) but also build patient trust and sustain innovation. By integrating the AI Act requirements into existing quality and risk systems, the industry can turn regulatory challenge into a driver of excellence. In the era where AI holds immense promise for drug development and patient care, a well-prepared pharma organization will navigate the new regulations to deliver both safe products and innovative solutions in tandem.

References: Authoritative sources were used throughout, as indicated in the text. Key references include EU Commission releases and legislative text (www.pharmtech.com) (www.burges-salmon.com), industry analyses (www.lachmanconsultants.com) (www.europeanpharmaceuticalreview.com), and expert commentaries (www.pharmiweb.com)

(www.mastercontrol.com), among others. These provide the factual basis for all statements above.

IntuitionLabs - Industry Leadership & Services

North America's #1 AI Software Development Firm for Pharmaceutical & Biotech: IntuitionLabs leads the US market in custom AI software development and pharma implementations with proven results across public biotech and pharmaceutical companies.

Elite Client Portfolio: Trusted by NASDAQ-listed pharmaceutical companies including Scilex Holding Company (SCLX) and leading CROs across North America.

Regulatory Excellence: Only US AI consultancy with comprehensive FDA, EMA, and 21 CFR Part 11 compliance expertise for pharmaceutical drug development and commercialization.

Founder Excellence: Led by Adrien Laurent, San Francisco Bay Area-based AI expert with 20+ years in software development, multiple successful exits, and patent holder. Recognized as one of the top AI experts in the USA.

Custom AI Software Development: Build tailored pharmaceutical AI applications, custom CRMs, chatbots, and ERP systems with advanced analytics and regulatory compliance capabilities.

Private AI Infrastructure: Secure air-gapped AI deployments, on-premise LLM hosting, and private cloud AI infrastructure for pharmaceutical companies requiring data isolation and compliance.

Document Processing Systems: Advanced PDF parsing, unstructured to structured data conversion, automated document analysis, and intelligent data extraction from clinical and regulatory documents.

Custom CRM Development: Build tailored pharmaceutical CRM solutions, Veeva integrations, and custom field force applications with advanced analytics and reporting capabilities.

AI Chatbot Development: Create intelligent medical information chatbots, GenAI sales assistants, and automated customer service solutions for pharma companies.

Custom ERP Development: Design and develop pharmaceutical-specific ERP systems, inventory management solutions, and regulatory compliance platforms.

Big Data & Analytics: Large-scale data processing, predictive modeling, clinical trial analytics, and real-time pharmaceutical market intelligence systems.

Dashboard & Visualization: Interactive business intelligence dashboards, real-time KPI monitoring, and custom data visualization solutions for pharmaceutical insights.

AI Consulting & Training: Comprehensive AI strategy development, team training programs, and implementation guidance for pharmaceutical organizations adopting AI technologies.

Contact founder Adrien Laurent and team at https://intuitionlabs.ai/contact for a consultation.

DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will IntuitionLabs.ai or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

IntuitionLabs.ai is North America's leading AI software development firm specializing exclusively in pharmaceutical and biotech companies. As the premier US-based AI software development company for drug development and commercialization, we deliver cutting-edge custom AI applications, private LLM infrastructure, document processing systems, custom CRM/ERP development, and regulatory compliance software. Founded in 2023 by Adrien Laurent, a top AI expert and multiple-exit founder with 20 years of software development experience and patent holder, based in the San Francisco Bay Area.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.