# Pharma AI Vendor Due Diligence: A Validation Checklist

By Adrien Laurent, CEO at IntuitionLabs • 2/14/2026 • 45 min read

pharma ai · vendor due diligence · ai validation · gxp compliance · fda regulations · life sciences · machine learning · data security · risk assessment

# Executive Summary

As artificial intelligence (AI) rapidly transforms pharmaceutical R&D, manufacturing, and commercialization, life science companies are increasingly turning to AI vendors to gain competitive advantage. Yet the promise of AI often collides with reality: vendor marketing ploys, unverified performance claims, and complex regulatory constraints frequently lead to unmet expectations or outright failures. Consequently, pharmaceutical buyers must conduct **rigorous due diligence** to validate AI vendor claims before signing contracts or deploying solutions. This report delivers a comprehensive checklist and framework for that due diligence, tailored to the unique requirements of the pharmaceutical industry.

Key findings and recommendations include:

- **Heightened Stakeholder Scrutiny**: AI is now an "immediate priority" for most Big Pharma (85% see AI as urgent ([1] www.fiercepharma.com)), yet analysts warn of "overheated marketing" and hype surrounding AI drug discovery ([2] www.statnews.com). Buyers must reconcile optimism with skepticism by demanding evidence for all vendor claims and by involving multidisciplinary stakeholders (R&D scientists, regulatory, IT, etc.) in evaluations ([3] www.clinicalleader.com) ([4] www.pharmoutsourcing.com).
- **Data & Model Transparency**: Vendors must disclose core details about data sources and model validation. Domain-specific AI (trained on pharmaceutical/clinical data) vastly outperforms generic AI on life-sciences tasks ([5] discover-pharma.com). Buyers should insist on documentation of model training, versioning, and performance metrics on representative data ([6] www.pharmaceuticalonline.com) ([7] pmc.ncbi.nlm.nih.gov).
- **Regulatory Compliance**: AI tools in pharma often fall under regulations (e.g. FDA, EMA, GxP, HIPAA). Buyers should verify that vendors follow relevant guidelines: e.g. FDA's AI/ML draft frameworks, GAMP 5, and ISO standards for medical devices and software. Audit trails, validation documents, and risk assessments are critical ([8] www.pharmaceuticalonline.com) ([9] pmc.ncbi.nlm.nih.gov).
- **Performance Verification**: Therapeutic decisions and manufacturing processes demand high accuracy. Vendors claiming high prediction accuracy must provide independent test results (not cherry-picked metrics). Performance metrics should be defined in advance and validated in multiple scenarios ([7] pmc.ncbi.nlm.nih.gov) ([10] www.medscape.com). Gatsby-case example: IBM Watson for Oncology famously produced "erroneous" treatment suggestions despite vendor hype ([11] www.medscape.com) ([10] www.medscape.com).
- **Bias and Ethics**: Pharma must ensure patient safety and equity. AI models trained on biased clinical data can produce discriminatory outcomes. Buyers should query vendors about bias testing and mitigation, and require transparency around datasets. For example, Watson's bias towards one cancer protocol was blamed on its training set bias ([12] medium.com).
- **Security & IP Protection**: Generative AI vendors often encourage customers to input confidential data. Contracts must explicitly restrict vendor reuse of sensitive prompts ([13] pharmaphorum.com). Buyers should check encryption standards (e.g. HIPAA compliance, ISO 27001), incident response plans, and segregated data environments ([13] pharmaphorum.com) ([14] www.clinicalleader.com).
- **Contractual Safeguards**: Vendors typically aim to limit liability. Pharma buyers should negotiate strong indemnities, performance-based Service Level Agreements (SLAs), and clear IP ownership. They should demand vendors maintain professional liability insurance and agree to rapid correction of failures ([15] innovaccer.com) ([16] pharmaphorum.com).
- **Implementation and Change Management**: Even the best AI can fail without user buy-in. Case studies show that tools without alignment to scientists' workflows go unused ([4] www.pharmoutsourcing.com) ([17] www.pharmoutsourcing.com). Due diligence should include pilot studies and UX evaluations to ensure tools meet real needs.

This report develops these findings into a structured **due diligence checklist**, supported by academic and industry sources. We analyze historical and current examples, discuss regulatory/risk contexts, and outline future trends. Tables summarize key questions buyers should ask. In sum, responsible AI procurement in pharma demands depth: verifying technical claims, ensuring compliance, and safeguarding patient and corporate interests.

# Introduction and Background

## The AI Imperative in Pharma

By 2026, AI has become ubiquitous in life sciences. Every major pharmaceutical firm is exploring AI for drug discovery, clinical trials, manufacturing, and even marketing. One survey found 70–85% of top pharma executives consider AI an "immediate priority" ([1] www.fiercepharma.com) and are increasing budgets for AI projects. Define Ventures reported that **85%** of Big Pharma leaders view AI as urgent, with over 80% raising AI spending ([1] www.fiercepharma.com). Use cases range from *in silico* drug screening to automating regulatory paperwork and mining real-world evidence. Analysts estimate that scaled AI could generate **$254 billion** in extra annual profits for pharma by 2030 ([18] www.baringa.com).

However, with massive hype comes risk. Stat News highlights an "unending stream of overheated marketing" in AI drug discovery, stressing that vendors often promise breakthroughs that may arrive years later or never ([2] www.statnews.com).A 2024 industry survey found 83% of pharma professionals called AI "overrated," despite widespread deployment ([19] www.fiercepharma.com). Real-world AI implementation lags – a Gartner study shows while 92% of life science companies have pilots, only 30% have scaled more than six projects ([20] www.baringa.com). Many initiatives stall due to data issues or governance gaps, as analysts repeatedly note ([20] www.baringa.com) ([9] pmc.ncbi.nlm.nih.gov).

Standard due diligence processes (e.g. vendor questionnaires, tech evaluations) often fail to capture AI-specific risks. AI-enabled tools are not like typical software; they may rely on opaque models trained on proprietary data, produce unpredictable outputs (hallucinations), or degrade with data drift ([6] www.pharmaceuticalonline.com) ([7] pmc.ncbi.nlm.nih.gov). Pharma's regulatory environment further complicates matters: Good Manufacturing Practice (GMP) guidelines now require "validation" of AI systems, treating data and algorithms as controlled assets ([6] www.pharmaceuticalonline.com) ([9] pmc.ncbi.nlm.nih.gov).

In this climate, a pharma-buying organization must **"trust but verify"** every claim an AI vendor makes ([6] www.pharmaceuticalonline.com). This report provides the historical context, current best practices, and future outlook for that verification process. We draw on peer-reviewed studies, regulatory guidelines, industry reports, and expert commentary to assemble a detailed AI due-diligence checklist specifically for pharmaceutical applications.

## Defining AI Vendor Claims and Due Diligence

AI vendors may claim a wide array of capabilities: e.g., "90% accuracy in safety signal detection," "FDA-compliant regulatory review," "natural language experts for clinical documentation," or "halving drug screening time." Each claim carries assumptions about data, algorithms, and context. Due diligence is the systematic process of testing those assumptions and gathering evidence to substantiate (or refute) the claims. It spans multiple domains:

- **Technical validation** of algorithms and data (model performance, robustness, data provenance).
- **Regulatory and compliance assessment** (alignment with FDA/EMA guidance, data privacy laws).
- **Security assessment** (cybersecurity posture, data protection mechanisms).
- **Business and legal review** (vendor's track record, contractual terms, liability).

In regulated pharma, due diligence is not optional. Unvalidated AI can result not only in business loss but also patient harm, regulatory violations, intellectual property leakage, or litigation. A rigorous AI vendor due diligence process protects all these interests.

In the following sections, we dissect each dimension of due diligence. We include multiple perspectives (legal, technical, business, and user) and illustrate with examples. Citations are provided for all substantive points. For clinicians or managers new to AI, we begin with a primer on the stakes and recent learnings, before diving into specific checklist items.

# The AI Hype Cycle and Pharma Context

## From Snake Oil to Strategy: Understanding Vendor Hype

Artificial intelligence remains a buzzword in pharma – and like all buzzwords, it risks attracting "snake oil" promises. Industry experts caution against accepting vendor marketing at face value. The press is replete with cautionary tales:

- **IBM Watson for Oncology**: Once touted as a technology able to provide personalized cancer treatment recommendations, Watson for Oncology later drew sharp criticism. During a 2018 STAT investigation, internal IBM documents revealed Watson often gave *"erroneous"* or *"unsafe"* cancer treatment advice ([11] www.medscape.com). In many cases, it was inaccurate or added no new insight beyond what doctors already knew ([21] www.medscape.com). Analysts noted that Watson was trained on a few synthetic cases rather than large real data sets ([22] www.medscape.com) ([23] www.medscape.com). Six years and billions invested later, independent reports concluded Watson had "not improved patient outcomes" ([21] www.medscape.com). This example shows that **promises of AI breakthroughs must be scrutinized**: vendor marketing does not guarantee clinical benefit. (For detailed case analysis, see [25]).

- **Generic vs Domain-Specific AI**: Another common pitfall arises from domain mismatch. Recent commentary emphasizes that *"generic, general-use AI models often fall short on pharma's complex data"* ([24] discover-pharma.com). Generic LLMs trained on books and websites may hallucinate or misinterpret medical records (e.g. confusing "physical activity level" with "wine drinking" ([25] discover-pharma.com)). By contrast, *purpose-built* models (trained on medical text and fine-tuned by clinicians) perform much better on clinical tasks ([5] discover-pharma.com) ([26] discover-pharma.com). Investors and buyers should therefore probe: are you licensing a custom pharmaceutical model, or a generic chatbot repackaged?

- **Over-Promising Results**: Pharma leaders report that many AI vendor success stories lack supporting data. The CEO of Insitro (a prominent AI biotech) warns that people *"think [AI] is going to happen tomorrow"* ([27] www.statnews.com), yet true breakthroughs remain years away. STAT's Casey Ross and Matthew Herper observe an "unending stream of overheated marketing" in AI drug discovery ([2] www.statnews.com). This echoes the broader tech phenomenon where startups tout "AI cures X in 50% less time" without peer-reviewed evidence.

The takeaway: buyers must adopt a critical stance. Any claim about accuracy, speed, or ROI should be verified against data and aligned with expert judgment. Marketing materials should be a starting point for investigation, not an endpoint of trust.

## Industry Adoption Trends and Skepticism

Despite skepticism, pharma's investment in AI has grown sharply. A 2025 survey of global pharma executives found **70–85%** of respondents deem AI an "immediate priority," with most expanding AI budgets ([1] www.fiercepharma.com). Companies are now pairing external vendors with internal initiatives; 40% combine in-house and vendor solutions ([28] www.fiercepharma.com).

However, the same survey notes that investment is targeted at "low-risk, high-efficacy" areas (like medical writing) initially ([29] www.fiercepharma.com). Pharma organizations remain quite cautious about high-risk applications. For example, an industry poll in late 2025 found **65% of regulatory-professionals distrust AI for generating compliance documents** ([30] www.fiercepharma.com). Their concerns included AI hallucinating content (40% worried about fabrications) and lack of audit trails (20%) ([31] www.fiercepharma.com). This suggests that pharma is not blindly adopting AI; rather, it is wary of mission-critical uses.

In practice, many companies create AI governance committees to oversee ethics and data policies. Define Ventures reported that ~80% of firms have dedicated AI governance structures in place ([32] www.fiercepharma.com). This governance environment underlines why due diligence is central: vendor decisions carry not just technical risk, but also ethical and compliance risk under these new oversight regimes.

# Core Areas of Due Diligence

To systematically evaluate an AI vendor, pharmaceutical purchasers should group questions into major domains. Below is a high-level outline; detailed criteria appear in subsequent sections and the accompanying tables.

1. **Technical Architecture and Model Validation**.

- *Questions*: How is the AI/ML model constructed? Is it proprietary, open-source, or a hybrid? What algorithms and features are used? Has the model been validated on independent test sets that resemble our data?
- *Rationale*: Transparent understanding of the model helps assess faith in claims. For example, if a vendor touts *95% accuracy*, know whether that is on training data, test data, or unseen clinical records. Validation must match intended use to avoid inflated metrics ([7] pmc.ncbi.nlm.nih.gov).

2. **Data Provenance and Quality**.

- *Questions*: What data was used to train and test the model? Is the vendor's data representative of our patient populations and therapeutic areas? How was data labeled and cleaned?
- *Rationale*: "Data is the foundation of AI" ([6] www.pharmaceuticalonline.com). Flawed or biased training data means flawed predictions. PHARMA buyers must ensure training sets meet ALCOA+ standards (Attributable, Legible, Contemporaneous, Original, Accurate, etc) ([33] www.pharmaceuticalonline.com) and correspond to the use-case population ([33] www.pharmaceuticalonline.com) ([34] medium.com).

3. **Performance Metrics and Testing**.

- *Questions*: What metrics does the vendor report (e.g. accuracy, AUC, precision/recall)? Are these metrics sensitive to class imbalance (common in safety data)? What are the false positive/negative rates?
- *Rationale*: Standard accuracy can be deceptive. In safety monitoring, for instance, serious events may be only 10% of cases ([35] www.vitrana.com). Vendors should provide balanced metrics and explain them in context ([7] pmc.ncbi.nlm.nih.gov).

4. **Regulatory Compliance and Validation**.

- *Questions*: Does the AI solution fall under medical device or software regulations (e.g. FDA's SaMD guidelines, EU Medical Device Regulation)? Has the vendor performed a Computerized System Validation or equivalent?
- *Rationale*: In regulated pharma, digital systems must be validated to show they are "fit for intended use" ([6] www.pharmaceuticalonline.com). For example, any AI used in pharmacovigilance must comply with GxP and CSV guidelines ([9] pmc.ncbi.nlm.nih.gov). Proper validation documentation is as important as technical performance.

5. **Security, Privacy, and Data Usage**.

- *Questions*: How does the vendor protect data? Are they HIPAA/GDPR compliant? What contractual rights do they claim to customer data and outputs (often a contentious issue with GenAI)?
- *Rationale*: AI systems often process sensitive IP (e.g. patient data, proprietary formulas). Contracts must explicitly restrict vendors from storing or reusing user data for other purposes ([13] pharmaphorum.com). Security certifications (SOC2, ISO 27001) and incident response plans are key evidence of maturity.

6. **Ethical Bias and Explainability**.

- *Questions*: Has the vendor tested for algorithmic bias across demographics (age, gender, ethnicity)? Does the AI provide explanations for decisions (e.g. feature importance, source references)?
- *Rationale*: Biased predictions can harm patient safety and violate regulations. For instance, Watson for Oncology produced recommendations skewed toward Memorial Sloan Kettering's practices ([12] medium.com). Buyers should

require descriptions of bias-mitigation strategies and evidence of explainability ([31] www.fiercepharma.com) ([25] discover-pharma.com).

7. **Business and Operational Fit**.

- *Questions*: How will the AI integrate into existing workflows (e.g. LIMS, SAP, EHR)? What changes or training will be needed? Does the vendor have references or prior deployments in pharma?
- *Rationale*: Even a high-performing model is useless if scientists won't use it ([4] www.pharmoutsourcing.com) ([17] www.pharmoutsourcing.com). A successful solution demands good UX design and alignment with user jobs. Also, as one due diligence framework notes, the ROI of an AI solution must be assessed in context of enterprise goals ([36] pmc.ncbi.nlm.nih.gov).

8. **Contractual and Legal Terms**.

- *Questions*: What warranties and liabilities does the vendor accept? Are service levels tied to performance (uptime, throughput)? Who owns the IP of model improvements? What happens if the vendor goes bankrupt or changes strategy?
- *Rationale*: AI vendors often try to limit liability for "model outputs". Pharma buyers must negotiate "skin in the game" – e.g. indemnities, insurance, and termination rights ([16] pharmaphorum.com) ([37] www.clinicalleader.com). Crucially, due diligence includes legal review to shift undue risk.

In the sections that follow, we delve into each pillar with detail and supporting evidence. We discuss the historical context of why each question matters (with examples), cite relevant guidelines and case studies, and suggest practical verification steps. Two summary tables at the end condense these considerations into actionable checklists.

# Background: Historical and Regulatory Context

Before diving into specifics, it is useful to review the evolving context of AI in pharma that shapes due diligence requirements.

## Regulatory Landscape

Pharmaceutical AI sits at the intersection of multiple regulatory domains:

- **FDA (USA)**: The FDA treats many clinical AI tools as Software-as-a-Medical-Device (SaMD). Draft frameworks for AI/ML-based SaMD emphasize *"data lineage, traceability, and ongoing performance monitoring"* ([8] www.pharmaceuticalonline.com). The FDA's proposed AI Action Plan encourages pre-certification and model transparency, though full regulations are still evolving.

- **EMA and International**: The European Medicines Agency has a reflection paper on big data and AI that *"stresses transparency, human oversight, and governance across the lifecycle"* of AI systems ([8] www.pharmaceuticalonline.com). The EU's upcoming AI Act likely will classify medical AI as "high-risk," imposing strict requirements. Likewise, national bodies (e.g. MHRA in the UK) are issuing guidance on algorithmic management.

- **GxP and GAMP**: Even if an AI tool is not an FDA-regulated device, pharmaceutical quality systems apply: GAMP 5 and FDA CFR Part 11 rules (e.g. electronic records) still require that computerized systems be validated. As one expert stresses, *"What hasn't changed is our duty to demonstrate that systems are fit for intended use, protect patients, and ensure data integrity."* ([38] www.pharmaceuticalonline.com). In practice, AI validation means demonstrating model performance and change control, akin to traditional software validation but with attention on data integrity and model drift ([39] www.pharmaceuticalonline.com) ([40] www.pharmaceuticalonline.com).

- **Data Privacy**: AI tools often process patient or health data, triggering HIPAA (US) or GDPR (EU) safeguards. Regulators (e.g. HHS OCR, FTC) mandate data protection impact assessments for novel AI applications. Data used for model training must be obtained with proper consent and de-identification, and usage rights clearly defined in contracts ([13] pharmaphorum.com) ([41] www.clinicalleader.com).
- **Liability Rules**: Traditionally, medical device errors incur severe liability. The EU is extending product liability laws to cover algorithms, and there are proposals for an AI-specific liability directive. Pharma buyers should note that, unlike in classical software, vendors may be held accountable for AI-driven decisions. Many vendors try to contractually limit this liability; due diligence must ensure reasonable risk-sharing ([42] pharmaphorum.com) ([16] pharmaphorum.com).

Regulatory guidance also highlights specific due diligence needs. For example, pharmacovigilance guidelines make clear that if AI is used for adverse event assessment, the AI system must follow CSV principles in the style of GAMP ([9] pmc.ncbi.nlm.nih.gov). The International Society for Pharm. Engineering (ISPE) suggests treating AI training pipelines like controlled systems under Annex 11 and Part 11 ([8] www.pharmaceuticalonline.com).

Given this complex tapestry of regulations, a holistic due diligence cannot neglect compliance. Evaluators should map each claim to relevant laws and guidelines. For instance, if a vendor claims its AI is “FDA approved” for labeling, the buyer must check 510(k) or de novo clearance records. If a tool uses patient data, one should verify that consent forms allow the usage described and that data flows comply with privacy rules. The drug industry’s rigorous audit culture demands documentation of all AI validation steps.

## Complexity of AI-Pharma Sector

Investors and analysts note that pharma AI is exceptionally complex. One industry article bluntly states: *“AI-Pharma companies are 100 times as complex as FinTech companies. Methodologies used to assess them should be 100 times as rigorous.”* ([43] healthmanagement.org). Why? Developing AI for drug discovery integrates biology, chemistry, regulatory science, and cutting-edge machine learning. Senior pharma technologists often describe AI startups as mysterious “black boxes” to outside investors ([44] healthmanagement.org). Even venture capitalists have had to devise new due diligence frameworks for AI-driven biotech, assessing hundreds of parameters describing technical maturity, team expertise, data assets and regulatory strategy ([45] healthmanagement.org).

For the buyer (who is not selling but procuring AI systems), similar scrutiny is warranted. Unlike purchasing a chemical reagent, deploying an AI model means betting on intangible algorithms and data pipelines. Poor diligence can easily lead to a solution that **“technically works but doesn’t meet user needs”** as one expert warns ([4] www.pharmoutsourcing.com) ([17] www.pharmoutsourcing.com).

This guide takes that advice to heart: we advocate deep, cross-disciplinary review of AI vendors in pharma. It is only by understanding the scientific and regulatory intricacies, alongside technical performance, that a buyer can legitimately trust an AI product.

# Technical Due Diligence

This section addresses core technical claims: data, model, and performance. We advise on how to evaluate the **algorithmic validity** of an AI vendor’s offerings.

## Data Quality and Scope

**Key Questions**: What datasets underlie the AI tool? Have they been independently audited for accuracy? Are they representative of the intended patient population, therapeutic areas, or laboratory environment? Were the data collected ethically and in compliance with regulations?

**Why It Matters**: In AI, the adage "garbage in, garbage out" is literally true. Pharmaceutical data often present challenges: small sample sizes, noisy lab records, heterogeneous sources (electronic health records, genomic assays, real-world evidence, etc.). Generic data cleaning tools may not suffice. As COVID vaccine developer Moderna has noted, differences in data format or quality can completely mislead models when scaled ([9] pmc.ncbi.nlm.nih.gov).

Regulators implicitly demand high data integrity. The ALCOA+ framework, borrowed from traditional pharma practices, applies to training data: every datum should be attributable, accurate, original, etc. ([33] www.pharmaceuticalonline.com). Buyers should insist vendors document data lineage (where each record came from) and handling (how it was normalized, anonymized, etc.).

In practice, ask vendors for:

- **Data Descriptions**: summaries of data sources, volumes, and types. E.g. if an AI monitors lab machines, which factories? If for text completion, what clinical notes or lab standards (CDISC, HL7) were used?
- **Data Audits**: reports on data quality control. Have they run sanity checks or bias audits (e.g. demographics of patient data)?
- **Coverage**: evidence that critical sub-populations or rare conditions aren't missing. For example, if an AI claims to classify side-effects, it should have been trained on ADE reports spanning the relevant geographies and patient demographics, or supplemented by synthetic cases if needed.

*(Example: The failure of Watson for Oncology stemmed partly from insufficient and skewed training data. IBM trained on synthetic case histories of only a few specialists, not on diverse real patient cases ([22] www.medscape.com). As a result, Watson's recommendations often did not align with standard practice at other hospitals ([46] medium.com).)*

Documented assurance of data integrity aligns with GxP: systems must have traceable input/output records. If possible, the buyer may request a *Data Protection Impact Assessment (DPIA)* or similar from the vendor that clarifies legal bases for each dataset.

## Model Architecture and Validation

**Key Questions**: How is the AI model built and validated? Are the underlying algorithms explained? Have external experts reviewed or replicated the results? Is there version control and retraining governance for the model?

**Why It Matters**: Models in pharma AI range from simple statistical regressions to deep neural networks or ensemble methods. The choice of technique impacts transparency and robustness. A heuristic is: *"more complex ≠ always better"*. For example, a random forest might suffice for batch process optimization, whereas drug imaging may require convolutional nets.

Buyers should inquire:

- **Model Type**: Ask if it's supervised learning, unsupervised, reinforcement, etc. If it is a neural net, is the architecture described (e.g. layers, hyperparameters)?
- **Training Process**: How was the model trained? Was the training hyperparameter search automated or manual? What computing resources (GPU clusters, distributed training) were used?
- **Validation Data Split**: Very importantly, were training/validation/test sets strictly separated? If robust machine learning practices are followed, there should exist held-out test sets never seen during development, preventing "data leakage" ([6] www.pharmaceuticalonline.com) ([7] pmc.ncbi.nlm.nih.gov). The vendor should commit that any performance metrics are from fresh test data.
- **Reproducibility**: Ideally, the buyer should have confidence that the results are reproducible. That could mean obtaining a technical appendix or whitepaper describing the algorithm, or even requesting a joint workshop where vendor data scientists demonstrate training on a subset of data.

If the vendor has published results (e.g. in a journal or conference), review those publications. Independent benchmarking (e.g. via Kaggle challenges or known datasets) can be telling: did the model truly beat existing baselines on problems similar to yours?

*(For example, many so-called "AI" drug candidates are never peer-reviewed; investors and buyers should be skeptical of unfounded claims until results appear in trusted journals or are validated in independent trials.)*

### Performance Metrics

Evaluation of an AI model's performance must go beyond headline accuracy. Key due diligence steps include:

- **Define Appropriate Metrics**: Ensure that metrics match the use case. For classification tasks with class imbalance (common in safety signal detection, where adverse events are rare), accuracy alone can be misleading ([35] www.vitrana.com). Prefer metrics like Area Under ROC (AUC), F1-score, or recall at a fixed precision. For predictive models in medicine, sensitivity (catching true positives) may be more critical than overall accuracy. Vendors should justify why chosen metrics reflect business needs, and provide confusion matrices if possible.
- **Benchmarking and Baselines**: Insist on comparisons to baseline methods. If a vendor claims "AI algorithm identifies compounds 50% faster," they should compare against conventional methods (statistical models, or manual lab screening). Similarly, if the vendor touts error rates, have they been compared to human performance or other algorithms?
- **Stress Testing**: Robustness tests, such as running the model on out-of-distribution data or introducing noise, can reveal reliability. Buyers might request a summary of such tests. Regular performance monitoring (e.g., tracking AUC drift over time) is also key, as data and real-world conditions change ([47] www.pharmaceuticalonline.com).

Citing specifics: the pharmacovigilance literature and FDA guidances stress that *"performance metrics must be proactively defined given the system's intended use"* ([7] pmc.ncbi.nlm.nih.gov). For high-risk tasks (diagnostics, patient dosing), vendors should specify error thresholds (e.g. maximum false negatives allowed) upfront ([48] www.pharmaceuticalonline.com) and document how performance was measured.

### Explainability and Transparency

**Key Questions**: Are model decisions explainable? If the model is a black box, what tools (like SHAP or LIME) does the vendor use to interpret outputs? Does the vendor provide documented reasoning or source references for AI-generated predictions?

**Why It Matters**: Pharma is highly risk-averse. Regulators and end users demand some level of rationale for AI decisions. For instance, if an AI suggests a drug motif, chemists want to know *why* (which structural features it "found" relevant). In clinical AI, physicians expect at least confidence scores or reference cases. Lack of explainability can kill trust: One survey reported 12.5% of regulatory professionals specifically worry about "opacity" in AI processes ([31] www.fiercepharma.com).

Due diligence tip: Ask for examples of explainability reports. For sample cases, does the AI output include tracebacks (e.g. source text snippets, or feature importances)? Verify consistency: if given the same input twice, does the model produce stable explanations? Some vendors claim to avoid "hallucinations" by design. Probe what that means technically.

*(Example: A healthcare AI platform might highlight the sentences of a medical text that triggered an AI diagnosis. The buyer should test if those highlights actually match clinical reasoning, rather than being random artifacts.)*

## Security and Data Protection

**Key Questions**: How does the vendor secure data in transit and at rest? Are there third-party security certifications? Does the vendor allow on-premises deployment or only cloud-based? How are encryption keys managed?

**Why It Matters**: Pharmaceutical data (clinical trials, molecular structures, patient info) are highly sensitive. Security breaches risk not just IP loss but regulatory fines and patient harm. AI vendors must demonstrate enterprise-level security:

- **Standards Compliance**: Look for ISO/IEC 27001, SOC 2 Type II, or FedRAMP certifications. These indicate formal security processes.
- **Infrastructure Controls**: Does the solution run on public cloud, private cloud, or on-premises? If cloud, which provider (AWS, Azure, etc) and region? For global operations, ensure data residency rules are respected.
- **Data Segregation**: The vendor should explicitly segregate each customer's data. Shared multi-tenancy must not allow data leakage.
- **Access Management**: Role-based access control, multi-factor authentication, and strict audit trails should be in place. Logging of user and system actions will be crucial for any investigation.

An often-overlooked risk is **model theft** or misuse. Proprietary ML models can be reverse-engineered if not protected. Buyers may request details on model encryption or obfuscation, especially if intellectual property must be guarded.

## Ethical Considerations and Bias

**Key Questions**: What steps has the vendor taken to identify and mitigate bias in their model? Are fairness audits conducted (e.g. checking performance across demographic groups)? Is there human-in-the-loop oversight for critical decisions?

**Why It Matters**: Biased AI can lead to harm: e.g., an ML model for dosing might perform poorly on underrepresented populations, endangering patient safety or reinforcing health disparities. In the Phillips vs. Maine hearing (hypothetical example), a biased AI recommendation could even lead to regulatory sanctions.

Actionable due diligence:

- **Bias Testing**: Request documentation that the model's predictions were evaluated across relevant subgroups (age, race, sex). For instance, if the AI predicts side-effect severity, does it perform equally well on all races? Bias audits should include confusion matrices per subgroup.
- **Data Diversity**: Review the training data's demographics. If crucial subpopulations are missing, the model is likely biased.
- **Human Oversight**: For high-stakes outputs, the vendor should specify how humans review AI suggestions. Ask for the interface design or SLAs addressing human review.

The clinical-leader commentary emphasizes "algorithmic bias and fairness" as part of due diligence ([49] www.mondaq.com). If a vendor claims a model is "industry proven" or "FDA quality," ensure those claims hold when considering bias: e.g., FDA may require evidence that a diagnostic AI was tested on a diverse clinical trial.

## Contractual and Service Considerations

**Key Questions**: Is the vendor stable (financially and operationally) enough to deliver long-term? What are the support and maintenance terms (patching, retraining, upgrades)? How will you ensure continuity if the vendor is acquired or exits the market?

**Why It Matters**: Unlike single-use lab equipment, AI is a service that often evolves. If a vendor disappears, the pharma company might be stranded with an unsupported algorithm embedded in critical processes. Contract terms must handle this:

- **Vendor Viability**: Perform company due diligence – funding, years in business, core investors. For small startups, the risk is higher; ensure escrow of code or a plan for technology transfer.
- **Service Level Agreements (SLAs)**: SLAs should cover not only uptime (server availability) but also performance guarantees. For instance, an SLA might promise retention of >X% precision or cadence of model retraining.
- **Right to Audit**: Contracts should allow the pharma buyer to audit the vendor's practices periodically, including security and validation processes.
- **Data and Model Portability**: Upon contract termination, can the customer retrieve their data and model? For instance, risk-based contracts might require vendors to provide a cleaned snapshot of the AI model's learned parameters to facilitate handover.
- **Liability and Indemnity**: As noted, vendors will cap liability. Buyers should secure indemnification clauses for IP infringement and data breaches, and push for broader coverage especially if the AI decision-making could cause patient harm.

Legal advisors should review all terms meticulously, given the evolving nature of AI liability. The checklist in Table 2 (later) lists specific contract clauses to watch.

# Case Studies and Illustrative Examples

In this section we highlight a few real-world scenarios that illuminate the importance of due diligence (or consequence of neglecting it).

## Case 1: Watson for Oncology (Published Example)

IBM Watson for Oncology (WFO) was one of the highest-profile cases of AI in pharma that ended poorly. IBM had struck a 2012 partnership with Memorial Sloan Kettering to train Watson on oncology guidelines, projecting that Watson would "analyze patient data against thousands of historical cases" ([50] www.medscape.com). After much hype, a 2018 STAT investigation revealed stark issues: Watson's recommendations were often *"erroneous or incorrect"*, and internal teams flagged "unsafe" advice ([11] www.medscape.com). It turned out Watson had been trained on only a handful of synthetic cases per cancer type rather than large real datasets ([22] www.medscape.com) ([23] www.medscape.com). As a result, when deployed, it either gave irrelevant suggestions or none that aligned with actual clinical protocols.

Key lessons relevant to due diligence:

- **Scrutinize Training Data**: WFO's failures traced to insufficient training examples. Buyers should ask vendors for summary statistics of their training sets. For example, how many annotated medical images or patient charts were used? Are they from the same clinical practice setting?
- **Demand Independent Verification**: No published studies at the time demonstrated that WFO improved care. Buyers should look for independent third-party validations. If none exist, be skeptical of vendors' internally reported accuracy.
- **Beware of Extrapolation**: WFO was touted as universally applicable, but in reality recommendations clashed with local formularies or patient demographics. Vendors should be clear about the intended geographic and clinical context of their tool. A due diligence step is asking: "For which populations or guidelines was this tested?"

Ultimately, Watson Health struggled and was divested in parts after billions invested ([51] www.medscape.com). IBM's example underscores that even tech giants' claims must be validated by purchasers.

## Case 2: Generative AI for Regulatory Submission

An emerging trend is using Large Language Models (LLMs) to draft regulatory documents or medical summaries. Suppose a vendor claims their LLM can generate Approved Label changes 10× faster. A due diligence tester should:

- Request examples of actual regulatory documents drafted by the tool and independently reviewed. Check for hallucinations or unsupported claims.
- Ask if the vendor's LLM was fine-tuned on regulatory filings (vs. generic text). If not, domain mismatch is likely to cause errors (as the Klick Health survey suggests, pharma experts largely distrust AI-generated compliance materials ([30] www.fiercepharma.com)).
- Verify control measures: e.g., does the tool include audit trails showing exactly which text was AI-generated and which was human-approved? Are draft edits tracked?

In one reported survey, 65% of pharma compliance professionals said they would *not* trust AI to create regulatory submissions ([30] www.fiercepharma.com). Key concerns were hallucinations (40%) and lack of auditability ([31] www.fiercepharma.com). A due diligence checklist should explicitly include testing the AI on compliance tasks to ensure no factual mistakes are "buried" in fine print, and requiring traceable provenance for every sentence.

## Example: Screening for Adverse Events

Consider a vendor claiming an AI model can flag serious adverse event (SAE) reports with 95% precision, reducing case intake work by half. Due diligence would involve:

- **Data Bias**: The vendor must clarify whether their training data included balanced examples of different SAEs. If 90% of training cases are head trauma and only 1% are rare cardiovascular events, the model might overlook the rare but critical cases (high false negatives). The buyer should see confusion matrices per event type.
- **Metric Dissection**: Precision of 95% sounds good, but what about recall? If the model avoids false flags (high precision) by only catching obvious cases, it may miss many real SAEs (low recall). For patient safety, recall (sensitivity) can be more critical in pharmacovigilance. Buyers should demand both precision and recall figures ([7] pmc.ncbi.nlm.nih.gov).
- **External Audit**: Ideally, the buyer would test the model on known datasets. For example, take 100 adjudicated SAE reports (with known outcomes) from internal archives, and evaluate model predictions. Did the model flag them correctly? Only with such in-house testing can vendor claims be validated.

As [45] emphasizes, any PV AI system *"must be validated"* under GxP ([9] pmc.ncbi.nlm.nih.gov). Thus, simply trusting a vendor's "95%" claim without seeing the validation protocol would violate best practices.

# Legal, Compliance, and Contractual due diligence

AI vendor claims often carry legal and compliance implications. Due diligence must therefore include a thorough review of legal risk.

## Contractual Protections and Liability

AI vendors try to protect themselves; buyers need to counterbalance:

- **Liability Caps**: Many AI contracts include liability caps that are grossly insufficient for life science consequences. Clients should negotiate higher caps, especially for breaches of warranty and indemnification. For instance, if an AI diagnostic misclassification leads to patient harm, the financial repercussions can be enormous. Vendors should bear responsibility for fundamental algorithmic errors. Pharmaceutical companies often require vendors to carry professional liability insurance for such risks ([15] innovaccer.com).

- **Indemnification**: Ensure the contract indemnifies the client from IP claims and data misuse. If an AI product inadvertently infringes a patent (e.g. by copying a patented molecule structure), the vendor should cover legal costs. Many vendors disclaim "open-source" dependencies; the contract must clarify who is liable if open-source code has a restrictive license or vulnerability.

- **Service Level Agreements (SLAs)**: Standard IT SLAs (99.9% uptime, response times) are necessary but not enough. For AI, include performance SLAs tied to outcome measures. For example, "If the model's accuracy on client-specific validation drops below X%, vendor will have 48 hours to remediate." Without such clauses, a covert model failure could trigger business disruption with no recourse.

- **Termination and Data Retrieval**: The contract should guarantee that upon project completion or termination, the pharma company retains rights to all produced data and knowledge. If the AI involved machine-learned parameters, the contract must allow exporting model weights or retraining using the customer's data alone (to avoid vendor "lock-in").

Legal experts note that buyer councils should *"know what laws apply and update contracts accordingly,"* citing HIPAA, HHS AI rules, etc. ([52] www.clinicalleader.com) ([41] www.clinicalleader.com). It is advisable to involve attorneys who specialize in AI or healthcare law, given how quickly regulations are evolving.

## Regulatory Compliance Clauses

Vendors should explicitly commit in contracts to follow applicable regulatory standards. For example:

- **Medical Device Regulations**: If the AI is a medical device (diagnostic, triage, etc.), vendor contract should affirm compliance with FDA QSR (or CE under MDR). It should confirm that the software has been validated under those regimes, and it should list any relevant regulatory approvals or filings. If none exist, that gap must be noted as a risk in the contract.

- **Data Protection**: Contracts must specify how data is handled, including data subject rights. For GDPR-covered data, the vendor is likely a "processor," and the contract must include standard data processing addendums. Clarify whether the vendor can use de-identified customer data for model improvement or benchmarking – or if they "shall not" use it beyond the agreed purpose ([13] pharmaphorum.com).

One recent article emphasizes that *"end-users will want to ensure the vendor has sufficient 'skin in the game' while users should not take on exposure the vendor will not assume."* ([16] pharmaphorum.com). In practice, that means strong clauses on indemnities and warranties. Test whether the vendor is resistant to such negotiations – resistance can be a red flag as much as a technical flaw.

## Compliance With Existing Guidance

Finally, due diligence should verify whether the AI vendor already complies with or references known oversight frameworks:

- **GAMP5 and CSV**: As noted in [9], current pharma guidelines (Annex 11, Part 11, etc.) do not explicitly differentiate AI vs classic systems, but their principles still apply. Vendors should understand concepts like ALCOA+ and demonstrate them in practice (audit trails, version control, etc.) ([6] www.pharmaceuticalonline.com) ([33] www.pharmaceuticalonline.com).
- **FDA Draft Guidelines**: If the tool is in a domain where FDA has draft guidance (e.g. lab testing, radiology), check the vendor's position. For instance, the FDA's AI framework draft emphasizes *"total product lifecycle"* monitoring – vendors should be prepared to implement performance monitoring dashboards as required ([47] www.pharmaceuticalonline.com).

- **Privacy Laws**: Ensure contract and practice align with HIPAA/HITECH (US), PIPEDA (Canada), or equivalent. For generative AI, confirm that PHI is not being fed into public LLMs inadvertently – or if it is, that Business Associate Agreements are in place. The FiercePharma article notes that many companies have outright banned ChatGPT use to avoid unsanctioned data leakage ([53] www.fiercepharma.com).

Legal due diligence is not merely checking boxes; it is about aligning contractual risk with business risk in a complex, shifting legal environment. Engaging in-depth with legal counsel is critical here.

# Security and Privacy Due Diligence

Given pharma's IP sensitivity and data protection obligations, buyers must rigorously vet vendor security.

## Data Usage and Privacy

For AI vendors, data flows are often contentious:

- **Data Ownership**: The original data (e.g. patient records, chemical libraries) should unequivocally remain the property of the pharma company. Even if used to train the model, the vendor must commit that ownership does not transfer. The contract should specify that any model outputs generated belong exclusively to the client (and vice versa, the vendor owns its model's underlying code).
- **Use of Customer Data**: Many AI platforms sneak in clauses allowing the vendor to use customer data to improve the vendor's broader models. In pharma, this is usually unacceptable if it involves de-identified health info. Buyers should prohibit any use of client data beyond the contracted service. If the vendor needs data to fine-tune the model, it must be done only on de-identified or synthetic data as approved by the client.
- **GenAI Prompt Data**: As highlighted in [16], generative AI vendors often claim rights over prompts or outputs. If the pharma scientist enters trade secrets or private formulas as prompts, the vendor must not repurpose them. ([13] pharmaphorum.com). Inspect contracts for "Training Data Rights" clauses and insist on strict limitations.

Practically, ask vendors:

- Do you store any customer-injected data (prompts, files) after use? For automated compliance, the answer should be "no" or "only within strict ephemeral buffers."
- How do you ensure PHI is not exposed (e.g. via misconfiguration or bugs)? The vendor must have clear data deletion and retention policies.

New regulations, like Europe's GDPR and the proposed U.S. HIPAA AI Rule, make data governance not just best practice but legal imperative. Documentation of data flows and privacy impact assessments should be part of diligence evidence.

## Cybersecurity Measures

High-level security questions include:

- **Standards and Audits**: Does the vendor undergo penetration testing and vulnerability assessments? Are third-party audit summaries available (SOC2 reports or ISO 27001 certificates)? Ideally, review these for any critical findings (major vulnerabilities or deficiencies).
- **Network Security**: Are all services encrypted in transit (e.g. TLS/SSL 1.2+)? Is data at rest encrypted with customer-managed keys? If the AI solution includes a web interface, does it use modern authentication (SAML, OAuth, MFA)?
- **Incident Response**: Has the vendor had any breaches? What is their incident response plan? Can the buyer get notifications within agreed timeframes if an incident occurs? The contract should define breach reporting deadlines (often 24–72 hours).

- **Supply Chain Security**: Many advanced AI tools rely on open-source libraries and third-party components. Request a Software Bill of Materials (SBOM) if possible. Ensure the vendor monitors dependencies for vulnerabilities (e.g. Spectre/Meltdown, Log4Shell) and has patching protocols.

Even if a vendor assures “we’re secure,” probing these details is essential. Sensitive IP leaks can create irreversible harm. One should treat AI vendors like any critical IT vendor – require compliance with the company’s procurement security policies (for example, hitting minimum security scorecards, as is done with cloud providers).

# Performance and Integration Considerations

Beyond validating claims in isolation, a pharma buyer must examine how the AI will actually work within the organization.

## Proof-of-Concept and Pilot Testing

A best practice is conducting a small-scale proof of concept (POC) or pilot using real data. This accomplishes several goals:

- **Testing Vendor Claims**: The vendor’s marketing metrics can be verified on a subset of the company’s own data. If a customer has historical data labeled by experts, running the AI on it can reveal performance gaps.
- **User Feedback**: Clinicians or scientists can trial the tool in a controlled environment. Their feedback will uncover usability issues early on. One pharma found that even though an AI could technically retrieve documents, scientists abandoned it when they couldn’t phrase queries in the “right” way ([54] www.pharmoutsourcing.com).
- **Integration Feasibility**: The POC often highlights practical hurdles. For instance, does the AI require data in a particular format (CSV vs. relational)? Does connecting to the corporate data warehouse require custom ETL work?

Before committing, ensure the POC has a defined “success criteria” agreed upon by both sides (e.g. “tool must correctly classify 90% of validation cases by day 10”). Document the process and results meticulously. This trial period can be part of contract negotiation (e.g. a conditional payment based on pilot success).

## Change Management and User Adoption

Even a powerful AI can fail without adoption. The Human Factors of AI include:

- **Usability/User Interface (UI)**: Is the tool intuitive? Pharma environments often have legacy interfaces and jargon. If an AI demands users learn new interfaces or complex commands, adoption stalls ([4] www.pharmoutsourcing.com) ([55] www.pharmoutsourcing.com). During due diligence, involve actual users (scientists, pharmacists, trial coordinators) and solicit their feedback on demos or mock-ups.
- **Explainability**: As noted, lack of transparency can erode trust ([56] www.pharmoutsourcing.com). In user testing, confirm that the system’s outputs are accompanied by explanations or confidence indicators that users can interpret. If an AI provides recommendations with no rationale, users are likely to reject or override them.
- **Training and Education**: Check that the vendor provides training materials tailored to pharma contexts. Who is included in training (clinical staff vs IT vs QA)? The vendor should offer robust documentation and ideally hands-on workshops. Per the Innovaccer blog, a good vendor will offer role-based training programs and support channels ([57] innovaccer.com).

If the due diligence process surfaces apprehension (e.g. “our team fears being replaced” ([58] www.pharmoutsourcing.com)), plan change management too. Some companies set up internal “AI champions” networks to pilot new tech and share successes, as recommended by Baringa ([59] www.baringa.com) ([60] www.baringa.com). Buyers should make this part of the engagement: not only check if the AI works, but if the organization *will* work with it.

# Implications and Future Directions

## Evolving Standards and Oversight

As of 2026, AI in pharma remains under intense development by regulators. Buyers should anticipate more formal standards forthcoming:

- **AI Act and FDA Guidance**: Within 2023–2025, regulators have signaled stricter rules for AI/ML. The EU AI Act is likely to categorize pharma predictive analytics as "high risk." That will mandate rigorous documentation, human oversight provisions, and possibly third-party certification. Over years, buyers may have to require vendors to comply with specific AI Act provisions (e.g. obligations for anomaly logging, risk assessment).
- **Industry Initiatives**: Organizations like ISPE, DIA, and IEEE are working on AI-specific guidance. For example, IEEE's proposed standard P7003 deals with bias considerations in medical AI. Keeping abreast of these can help structure future due diligence. Customers might cite such standards in RFPs.
- **Ongoing Performance Monitoring**: The view of AI as "set-and-forget" is shifting. Future due diligence will likely require systems for continuous monitoring: FDA and EMA emphasize that models should be tracked after deployment (to detect drift or data shifts) ([47] www.pharmaceuticalonline.com). Buyers may need to partner with vendors in setting up dashboards and retraining triggers.

## The Changing Vendor Landscape

Looking forward, the market for AI tools will both proliferate and consolidate. The building of bespoke models by Big Tech (like OpenAI/GPT-7 with pharma datasets) might provide alternatives to pure AI startups. Meanwhile, industry consortiums might pool resources for data sharing, which could empower incumbents.

For the due diligence checklist, this means:

- Expect an **autoregressive model**: vendor claims today may become outdated quickly. For example, if the vendor relies on GPT-4 for summarization today but next year open-source domain LMs match it, future buyers will expect ability to upgrade. Contracts and diligence should allow for technological updates.
- Open Source Impact: Many companies will incorporate open-source foundation models (e.g. Meta Llama or Hugging Face models). The checklist should incorporate open-source compliance (licenses, reproducibility) as a subitem.

As generative AI becomes more common, new risks like "prompt injection attacks," "model inversion," or "deepfake clinical data" may emerge. While beyond today's scope, forward-looking buyers should ask vendors how they are preparing for such threats. For instance, some are exploring on-device (edge) inference to avoid cloud exposure, or federated learning so models train on encrypted local data.

## Strategic Due Diligence

Overall, an AI vendor due diligence checklist should not be static. It must evolve with:

- **Company Strategy**: Align AI purchases with the strategic goals of the pharma enterprise. The npj framework recommends starting with strategic alignment and value case analysis ([36] pmc.ncbi.nlm.nih.gov). If an AI solution does not clearly tie into a quantifiable problem, it may not be worth detail scrutiny or investment.
- **Feedback and Learning**: Each AI procurement should inform the next. Successful due diligence builds organizational knowledge of "what good looks like" in AI tools. Tracking vendor performance post-deal (e.g. through KPIs) feeds back into the evaluation of future vendors.

In summary, **due diligence is an ongoing process**, interweaving technical assessment with legal review and change management. It requires significant effort, but given the stakes in pharma—patient safety, IP protection, and regulatory compliance—such rigor is warranted.

# Conclusion

Pharmaceutical companies stand at a crossroads with AI: the potential benefits are vast, from faster drug discovery to more efficient trials, but so are the risks. The past few years have shown that unvetted AI can lead to wasteful spending or, worse, patient harm. A rigorous, structured due diligence process is not just prudent; it is essential to responsibly harness AI in this domain.

This report has assembled a detailed "due diligence checklist" covering technical, regulatory, security, and operational dimensions, drawing on real-world examples and expert guidance. Key themes include:

- **Treat AI as a controlled system**: rigorously validate models against intended use, just as any GMP system would be.
- **Demand transparency**: insist on clarity about data, algorithms, and testing methodology. Claims of outsize performance require independent evidence.
- **Prioritize safety and compliance**: never accept vendor claims of "compliance" without documentation, and ensure all AI usage adheres to FDA/EMA and data protection rules.
- **Manage risk contractually**: use legal tools to align incentives, including performance-based SLAs and robust indemnities.
- **Engage users early**: test tools in pilot programs and confirm alignment with workflows to ensure adoption.

In the words of one AI governance expert: *"AI vendor relationships are not set-it-and-forget-it."* ([61] www.clinicalleader.com) As the regulatory landscape matures and AI technologies advance (e.g. with generative AI, edge AI, etc.), continuous vigilance will be needed. Future due diligence will likely involve new items (e.g. guardrails against synthetic data misuse, AI auditing by third parties).

Nevertheless, the core principle remains constant: **trust but verify**. With disciplined vetting of vendor claims, pharma companies can confidently integrate AI into their processes, unlocking value without sacrificing safety or compliance.

---

# References

All claims and recommendations above are supported by sources from industry reports, journal articles, and expert commentaries, as cited in the text:

- [9] Korrapati, "Trust But Verify: Validating AI in Pharma's GxP World", *Pharmaceutical Online*, Oct. 2025 (discussion of AI validation principles and regulatory expectations) ([8] www.pharmaceuticalonline.com) ([6] www.pharmaceuticalonline.com).
- [12] Sutten, Mike, "Ultimate AI Vendor Checklist for Healthcare Leaders", *Innovaccer Blog*, Feb. 2025 (technical, domain, risk, performance due diligence aspects) ([15] innovaccer.com).
- [14] Karofsky, E., "Why Pharma AI Projects Fail: The Human Problem Behind Technical Success", *Pharmaceutical Outsourcing*, Aug. 2025 (case series on adoption issues and UX importance) ([4] www.pharmoutsourcing.com) ([56] www.pharmoutsourcing.com).
- [15] Laws, L., interview with T. O'Connell, "Why generic AI fails pharma and the case for specialized AI", *Discover Pharma*, Jul. 2025 (expert discussion of domain-specific vs generic AI failures) ([25] discover-pharma.com) ([5] discover-pharma.com).

- [16] Pharmaphorum, *“10 legal risks to consider when implementing AI in pharma supply chains”* (Oct. 2025) (legal risks: data use, bias, liability, contractual safeguards) ([13] pharmaphorum.com) ([42] pharmaphorum.com).
- [18] O’Connor & Colgan Dunlap, “Advice on selecting your first AI-enabled vendor”, *Clinical Leader*, Dec. 2025 (Q&A on terms like algorithm transparency and necessary diligence steps) ([62] www.clinicalleader.com) ([14] www.clinicalleader.com).
- [20] Ruggio, M., “Due Diligence In AI Vendor Selection”, *Lexology/Mondaq*, Aug. 2024 (outline of due diligence focus areas: privacy, compliance, bias, liability) ([49] www.mondaq.com).
- [25] Nelson, R., “IBM Watson Oncology: Not Living Up to Expectations”, *Medscape*, Aug. 2018 (report on STAT and WSJ findings about Watson) ([11] www.medscape.com) ([21] www.medscape.com).
- [27] Ross, C. & Herper, M., “AI & drug discovery: separate hype from reality”, *STAT News*, May 2024 (quotes on AI hype in drug development) ([2] www.statnews.com) ([27] www.statnews.com).
- [30] Binkley et al., “An early pipeline framework for assessing vendor AI solutions to support ROI”, *npj Digit. Med.*, Jun. 2025 (governance framework for vendor AI selection) ([36] pmc.ncbi.nlm.nih.gov) ([63] pmc.ncbi.nlm.nih.gov).
- [34] Reddy et al., “Unlocking the business value from AI in Pharma”, *Baringa Whitepaper*, June 2025 (insights on data readiness, governance, and AI scaling) ([64] www.baringa.com) ([20] www.baringa.com).
- [39] HealthManagement, “Leveraging advanced methods to evaluate AI-Pharma companies”, May 2019 (commentary on complexity of AI in pharma) ([43] healthmanagement.org).
- [42] Becker, Z., “AI adoption is an ‘immediate priority’ to most Big Pharmas, report finds”, *FiercePharma*, Jul. 2025 (Define Ventures survey on AI adoption, budgets, governance structures) ([1] www.fiercepharma.com) ([32] www.fiercepharma.com).
- [43] Taylor, N. P., “Pharma pros skeptical of letting AI loose on regulatory compliance submissions: survey”, *FiercePharma*, Nov. 2025 (survey of pharma professionals on trust in AI for regulatory files) ([30] www.fiercepharma.com) ([31] www.fiercepharma.com).
- [45] [47] Huysentruyt et al., “Validating Intelligent Automation Systems in Pharmacovigilance”, *Drug Saf.*, Feb. 2021 (framework for AI validation in safety case processing) ([9] pmc.ncbi.nlm.nih.gov) ([7] pmc.ncbi.nlm.nih.gov).
- Additional sources were consulted for definitions and context (including AI industry blogs, LinkedIn insights, and emerging regulatory proposals), but the core points above are substantiated by the citations listed.

## External Sources

[1] https://www.fiercepharma.com/marketing/ai-tech-immediate-priority-most-big-pharmas-many-plan-open-their-pockets-further-ai#:~:The%2...

[2] https://www.statnews.com/2024/05/20/artificial-intelligence-drug-development-hype-reality-insitro/#:~:A%20r...

[3] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:What%...

[4] https://www.pharmoutsourcing.com/Featured-Articles/621020-Why-Pharma-AI-Projects-Fail-The-Human-Problem-Behind-Technical-Success/#:~:Despi...

[5] https://discover-pharma.com/why-generic-ai-fails-pharma-and-how-purpose-built-ai-is-revolutionizing-drug-development/#:~:There...

[6] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:Valid...

[7] https://pmc.ncbi.nlm.nih.gov/articles/PMC7892696/#:~:Requi...

[8] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:Regul...

[9] https://pmc.ncbi.nlm.nih.gov/articles/PMC7892696/#:~:work%...

[10] https://www.medscape.com/viewarticle/900746#:~:The%2...

[11] https://www.medscape.com/viewarticle/900746#:~:Howev...

[12] https://medium.com/%40bhavikadevjani/the-failure-of-ibms-watson-for-oncology-43f6787ff9a7#:~:patie...

[13] https://pharmaphorum.com/deep-dive/10-legal-risks-consider-when-implementing-ai-pharma-supply-chains#:~:Contr...

[14] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:inclu...

[15] https://innovaccer.com/resources/blogs/are-healthcare-organizations-evaluating-ai-vendors-correctly-before-signing#:~:They%...

[16] https://pharmaphorum.com/deep-dive/10-legal-risks-consider-when-implementing-ai-pharma-supply-chains#:~:Contr...

[17] https://www.pharmoutsourcing.com/Featured-Articles/621020-Why-Pharma-AI-Projects-Fail-The-Human-Problem-Behind-Technical-Success/#:~:Users...

[18] https://www.baringa.com/en/insights/pharma-ai/unlocking-the-business-value-from-ai-in-pharma/#:~:Artif...

[19] https://www.fiercepharma.com/marketing/ai-tech-immediate-priority-most-big-pharmas-many-plan-open-their-pockets-further-ai#:~:The%2...

[20] https://www.baringa.com/en/insights/pharma-ai/unlocking-the-business-value-from-ai-in-pharma/#:~:A%20G...

[21] https://www.medscape.com/viewarticle/900746#:~:Echoi...

[22] https://www.medscape.com/viewarticle/900746#:~:the%2...

[23] https://www.medscape.com/viewarticle/900746#:~:hours...

[24] https://discover-pharma.com/why-generic-ai-fails-pharma-and-how-purpose-built-ai-is-revolutionizing-drug-development/#:~:Why%2...

[25] https://discover-pharma.com/why-generic-ai-fails-pharma-and-how-purpose-built-ai-is-revolutionizing-drug-development/#:~:The%2...

[26] https://discover-pharma.com/why-generic-ai-fails-pharma-and-how-purpose-built-ai-is-revolutionizing-drug-development/#:~:Handl...

[27] https://www.statnews.com/2024/05/20/artificial-intelligence-drug-development-hype-reality-insitro/#:~:%E2%8...

[28] https://www.fiercepharma.com/marketing/ai-tech-immediate-priority-most-big-pharmas-many-plan-open-their-pockets-further-ai#:~:And%2...

[29] https://www.fiercepharma.com/marketing/ai-tech-immediate-priority-most-big-pharmas-many-plan-open-their-pockets-further-ai#:~:The%2...

[30] https://www.fiercepharma.com/marketing/pharma-pros-skeptical-letting-ai-loose-regulatory-compliance-submissions-survey#:~:promo...

[31] https://www.fiercepharma.com/marketing/pharma-pros-skeptical-letting-ai-loose-regulatory-compliance-submissions-survey#:~:The%2...

[32] https://www.fiercepharma.com/marketing/ai-tech-immediate-priority-most-big-pharmas-many-plan-open-their-pockets-further-ai#:~:Accor...

[33] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:1,unr...

[34] https://medium.com/%40bhavikadevjani/the-failure-of-ibms-watson-for-oncology-43f6787ff9a7#:~:The%2...

[35] https://www.vitrana.com/benchmarking-ai-solutions-in-pharmacovigilance-kpis-and-best-practices/#:~:,misl...

[36] https://pmc.ncbi.nlm.nih.gov/articles/PMC12170878/#:~:A%20r...

[37] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:To%20...

[38] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:cases...

[39] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:for%2...

[40] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:1,lev...

[41] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:Data%...

[42] https://pharmaphorum.com/deep-dive/10-legal-risks-consider-when-implementing-ai-pharma-supply-chains#:~:Produ...

[43] https://healthmanagement.org/s/leveraging-advanced-methods-to-evaluate-ai-pharma-companies#:~:The%2...

[44] https://healthmanagement.org/s/leveraging-advanced-methods-to-evaluate-ai-pharma-companies#:~:Due%2...

[45] https://healthmanagement.org/s/leveraging-advanced-methods-to-evaluate-ai-pharma-companies#:~:Deep%...

[46] https://medium.com/%40bhavikadevjani/the-failure-of-ibms-watson-for-oncology-43f6787ff9a7#:~:patie...

[47] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:1,min...

[48] https://www.pharmaceuticalonline.com/doc/trust-but-verify-validating-ai-in-pharma-s-gxp-world-0001#:~:Accep...

[49] https://www.mondaq.com/unitedstates/new-technology/1503766/due-diligence-in-ai-vendor-selection-a-cornerstone-for-healthcare-organizations#:~:,rela...

[50] https://www.medscape.com/viewarticle/900746#:~:STAT%...

[51] https://www.medscape.com/viewarticle/900746#:~:Gloom...

[52] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:conce...

[53] https://www.fiercepharma.com/marketing/ai-tech-immediate-priority-most-big-pharmas-many-plan-open-their-pockets-further-ai#:~:%E2%8...

[54] https://www.pharmoutsourcing.com/Featured-Articles/621020-Why-Pharma-AI-Projects-Fail-The-Human-Problem-Behind-Technical-Success/#:~:,the%...

[55] https://www.pharmoutsourcing.com/Featured-Articles/621020-Why-Pharma-AI-Projects-Fail-The-Human-Problem-Behind-Technical-Success/#:~:User%...

[56] https://www.pharmoutsourcing.com/Featured-Articles/621020-Why-Pharma-AI-Projects-Fail-The-Human-Problem-Behind-Technical-Success/#:~:You%2...

[57] https://innovaccer.com/resources/blogs/are-healthcare-organizations-evaluating-ai-vendors-correctly-before-signing#:~:Train...

[58] https://www.pharmoutsourcing.com/Featured-Articles/621020-Why-Pharma-AI-Projects-Fail-The-Human-Problem-Behind-Technical-Success/#:~:Even%...

[59] https://www.baringa.com/en/insights/pharma-ai/unlocking-the-business-value-from-ai-in-pharma/#:~:Imple...

[60] https://www.baringa.com/en/insights/pharma-ai/unlocking-the-business-value-from-ai-in-pharma/#:~:Scali...

[61] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:also%...

[62] https://www.clinicalleader.com/doc/can-t-miss-advice-on-selecting-your-first-ai-enabled-vendor-0001#:~:Algor...

[63] https://pmc.ncbi.nlm.nih.gov/articles/PMC12170878/#:~:essen...

[64] https://www.baringa.com/en/insights/pharma-ai/unlocking-the-business-value-from-ai-in-pharma/#:~:AI%E2...

## 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.

**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.