Can Life Sciences Companies Use Chinese AI Models Safely?

Published July 19, 2026 38 min read

Can Life Sciences Companies Use Chinese AI Models Safely?

Executive Summary

Life sciences companies can technically access Chinese artificial intelligence (AI) models such as **DeepSeek**, **Kimi K2/K3** from Moonshot AI, and **Qwen** from Alibaba, but whether they can do so safely and legally depends almost entirely on deployment mode, not on the model's country of origin alone. The distinction between a hosted chatbot operated on servers inside the People's Republic of China (PRC) and a self-hosted open-weight model run on the company's own infrastructure is, according to legal analysts, "the legal risk attaches to the service model, not just the model name" (Source: compound.law). DeepSeek's own privacy policy states plainly that the company will "directly collect, process and store your Personal Data in People's Republic of China" (Source: cdn.deepseek.com), which means GDPR-covered transfers to the hosted service require an applicable transfer mechanism, such as Article 46 safeguards, because China has no European Commission adequacy decision (Source: gdpr-info.eu). Italy's data protection authority, the Garante, ordered DeepSeek blocked nationwide within days of launch after finding the company's answers about its data practices "totally insufficient" (Source: reuters.com), and multiple German state data protection authorities have since escalated formal investigations against the service (Source: compound.law).

In the United States, the calculus is shaped less by a single "China ban" than by a stack of overlapping rules. The Department of Justice's Bulk Data Transfer Rule, which took effect April 8, 2025 under Executive Order 14117, prohibits or restricts transactions that give "countries of concern," a list that explicitly includes China, access to bulk sensitive American data, and it sets a specific threshold of more than 10,000 U.S. persons' worth of "personal health data" (Source: jacksonlewis.com), a threshold most clinical trial datasets and patient registries will exceed quickly. Separately, Texas became the first US state to restrict DeepSeek on government devices, followed within days by New York and Virginia (Source: insidegovernmentcontracts.com), and at least one bill in Congress, the "No DeepSeek on Government Devices Act," would codify a federal device ban (Source: congress.gov). The National Institute of Standards and Technology's Center for AI Standards and Innovation (CAISI) found in a formal evaluation that DeepSeek's most secure model responded to 94% of jailbreak attempts versus 8% for U.S. reference models, and that DeepSeek-based agents were twelve times more likely to follow malicious instructions than U.S. frontier models (Source: nist.gov) (Source: nist.gov).

For pharmaceutical, biotechnology, and medical device companies specifically, the analysis layers on top of general enterprise data governance. The U.S. Food and Drug Administration's (FDA) draft guidance on AI in regulatory submissions requires a risk-based credibility framework for any AI model used to support safety, effectiveness, or quality claims (Source: fda.gov), and the EU's AI Act, fully applicable as of August 2, 2026, classifies AI embedded in medical devices as high-risk, triggering conformity assessment obligations (Source: digital-strategy.ec.europa.eu). Under HIPAA, the Health and Human Services Office for Civil Rights has confirmed it will enforce nondiscrimination requirements against AI-based clinical decision tools (Source: reedsmith.com), and a Kiteworks-sponsored industry survey found only 17% of life science organizations have implemented automated controls to stop sensitive data leaking into AI tools of any origin (Source: contractpharma.com).

The bottom line: hosted Chinese chatbots and their consumer APIs (DeepSeek's web app, Kimi's public chat) are unsuitable for any workflow touching regulated personal, health, or genomic data, in the United States, the European Union, or under China's own strict data-export regime, which China's leading think tank analysis frames as pushing multinationals toward a "China-for-China" architecture (Source: atlanticcouncil.org). Self-hosted, open-weight deployments of models whose weights are actually available—such as DeepSeek-V3/R1, Kimi K2, and Qwen—can present a materially different risk profile when run on a life sciences company's controlled infrastructure with no data flowing to the developer. Kimi K3 was available through Moonshot's products and API as of July 26, 2026, but Moonshot said its full weights would be released by July 27, 2026; it should not yet be treated as a self-hosted option (Moonshot AI. These deployments still require the same GxP validation, security review, and vendor due diligence that any AI system requires in a regulated environment. This report walks through the deployment-mode taxonomy, the overlapping US, EU, and Chinese legal regimes, the life sciences-specific compliance layer, documented security and censorship findings, and a risk-based framework life sciences AI governance teams can apply today, as of July 2026.

Introduction and Background

The question of whether life sciences companies can use Chinese AI models became urgent almost overnight. When DeepSeek's R1 reasoning model launched on app stores on January 20, 2025, it triggered a market shock that wiped over $590 billion from Nvidia's market capitalization within a day and pushed the S&P 500 down more than 1.2% (Source: publications.lawschool.cornell.edu), because the Chinese startup claimed performance on par with leading US models at a small fraction of the reported development cost. Since then, Moonshot AI's **Kimi K2** (July 2025) and **Kimi K3** (July 2026, 2.8 trillion parameters, positioned by its developer as "the new frontier of intelligence" with native multimodality and a 1M-token context window) (Source: moonshot.ai), along with Alibaba's Qwen family, have extended the same pattern: capable, inexpensive, and often open-weight Chinese models that pharmaceutical, biotech, and medical device organizations are being asked to evaluate for drug discovery literature review, clinical documentation drafting, regulatory writing support, and general knowledge-work automation.

Life sciences organizations sit at the intersection of the most stringent data privacy regimes (GDPR, HIPAA) and the most stringent product regulation regimes (FDA, EMA, GxP quality systems) in the global economy. That dual exposure changes the calculus relative to, say, a retailer or a marketing agency experimenting with the same model. A pharmaceutical company's prompts may contain unpublished clinical trial results, proprietary molecular structures, or patient-level real-world data, exactly the categories the Kiteworks-sponsored industry study found employees routinely paste into generative AI tools of every origin, with 27% of life sciences organizations acknowledging that more than 30% of their AI-processed data is sensitive or private (Source: contractpharma.com).

This report is not a product comparison of AI vendors. It is an explainer aimed at compliance officers, IT security leads, and R&D informatics teams who must answer a specific question their leadership is asking: can we use DeepSeek, Kimi, or Qwen, and under what conditions? As an **adjacent advisor** to the life sciences industry rather than an AI model vendor, IntuitionLabs approaches this question from the perspective of an organization that helps pharmaceutical and biotech clients build AI governance and vendor due diligence programs, including for Veeva-adjacent regulated workflows, rather than one that sells or competes with any of the models discussed here. The analysis below draws on regulatory text, government evaluations, legal advisories, and the vendors' own published policies, all fetched and verified during this research, to build a defensible, risk-based answer.

Chinese AI Models in 2026: A Deployment-Mode Taxonomy

The single most consequential fact for any life sciences compliance analysis is that "Chinese AI model" is not one product category. It spans at least three distinct deployment modes, each with a different legal exposure, and conflating them is the most common analytical error compliance teams make.

Hosted consumer chatbots and public APIs. This is DeepSeek's mobile app and web chat, and Kimi's consumer chat product at kimi.com. Both route prompts to servers controlled by the Chinese developer. DeepSeek's privacy policy is explicit that the company will "directly collect, process and store your Personal Data in People's Republic of China" (Source: cdn.deepseek.com), and further states it uses submitted data "to train and improve

our technology, such as our machine learning models and algorithms" (Source: cdn.deepseek.com). This is the mode nearly every government restriction targets.

Vendor-hosted API access. DeepSeek, Moonshot AI (for Kimi), and Alibaba (for Qwen) all offer developer APIs that still route data through the vendor's infrastructure, though contractual terms and server locations differ meaningfully. Moonshot AI's own OpenPlatform privacy policy states that "our servers are situated in Singapore" and that "your personal data may be transferred to and stored on servers located outside your country of residence" (Source: platform.kimi.ai) (Source: platform.kimi.ai). That is a materially different jurisdictional footprint than DeepSeek's explicit PRC storage, but server location alone does not place a service outside GDPR or US regulatory reach. For GDPR-covered transfers, Singapore hosting remains subject to the applicable international-transfer analysis; US-law applicability depends on the parties, data flow, transaction type, and other statutory criteria (EDPB; US Department of Justice.

Self-hosted open-weight deployment. DeepSeek-V3/R1, Kimi K2, and Qwen have downloadable weights that an organization can run on its own infrastructure, in its own jurisdiction, without sending operational data to the original developer. Kimi K3 was not yet a self-hosting option as of July 26, 2026: Moonshot offered it through its products and API and said full weights would be released by July 27, 2026 (Moonshot AI. Moonshot AI's official GitHub repository confirms that "both the code and the model weights are released under the Modified MIT License" (Source: github.com), and describes the underlying architecture as "a state-of-the-art mixture-of-experts (MoE) language model with 32 billion activated parameters and 1 trillion total parameters" (Source: github.com). Alibaba's Qwen models are released under a mix of Apache 2.0 (for smaller variants) and a custom "Tongyi Qianwen LICENSE AGREEMENT" for larger models, as published in the official QwenLM repository (Source: github.com). This is the mode that legal analysts consistently describe as "a separate compliance scenario" from the hosted service, because "the legal risk attaches to the service model, not just the model name" (Source: compound.law).

Kimi K3, launched July 17, 2026 (Moonshot's fiscal 2026 as reported), extends this taxonomy: Moonshot AI described it as "the world's largest open AI model" at 2.8 trillion parameters (Source: forbes.com), while Moonshot AI itself, founded in 2023 and backed by Alibaba and Tencent, reached a valuation of more than $20 billion after raising roughly $2 billion in its latest funding round (Source: forbes.com), with annual recurring revenue that topped $200 million as of April 2026 (Source: forbes.com). K2's API pricing was set around $0.15 per million input tokens and $2.50 per million output tokens, a fraction of comparable Western frontier model pricing, according to IntuitionLabs' own technical analysis of the model family (Source: intuitionlabs.ai). That aggressive pricing, and the open-weight release model, is precisely why life sciences procurement teams keep asking about these models: the cost and capability case is compelling even where the compliance case is not straightforward.

Table 1 below summarizes the three deployment modes across the models most frequently proposed to life sciences buyers.

MODEL / DEVELOPER	HEADQUARTERS	LICENSE / OPENNESS	WHERE HOSTED DATA IS STORED	NOTABLE COMPLIANCE CONSIDERATION
DeepSeek (Hangzhou DeepSeek Artificial Intelligence Co.)	Hangzhou, China	V3 code is MIT-licensed; model weights are subject to DeepSeek's separate Model License, which includes use-based restrictions and other conditions; hosted app/API is a closed service	People's Republic of China, per DeepSeek's own privacy policy (Source: cdn.deepseek.com)	Blocked in Italy (Source: reuters.com); flagged by NIST CAISI for security and censorship risk (Source: nist.gov)
Kimi K2 (Moonshot AI)	Beijing, China	Modified MIT License for weights and code (Source: github.com)	Singapore for the hosted OpenPlatform service, per Moonshot's privacy policy (Source: platform.kimi.ai)	Singapore hosting does not itself determine GDPR or US-law applicability; assess the transfer and transaction
Kimi K3 (Moonshot AI)	Beijing, China	Hosted/API-only as of July 26, 2026; Moonshot said full weights would be released by July 27 (Moonshot AI	Available through Moonshot products and API	Do not treat as a self-hosted option until the weights are available
Qwen (Alibaba Cloud)	Hangzhou, China	Apache 2.0 for smaller variants; custom "Tongyi Qianwen" license for larger models (Source: github.com)	Hosted API (DashScope) processes data on Alibaba Cloud infrastructure; self-hosted deployment avoids this entirely	Permissive open-weight licensing makes self-hosting on domestic (US/EU) infrastructure comparatively straightforward

The table shows that data residency, not brand name, is the operative variable. A life sciences company that self-hosts DeepSeek-V3 weights on its own AWS GovCloud or EU-region infrastructure has a fundamentally different, and generally more defensible, risk profile than one whose employees log into deepseek.com from a corporate laptop. The same is true of Kimi and Qwen. This distinction recurs throughout every regulatory regime discussed below, and it is the first question any life sciences AI governance committee should ask before evaluating anything else about a proposed Chinese model deployment.

Data Sovereignty and Cross-Border Transfer Law

The GDPR problem. The European Commission maintains a list of "third countries" it deems to provide an adequate level of data protection, currently comprising "Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom and South Korea," plus certified US organizations under the EU-US Data Privacy Framework since July 10, 2023 (Source: gdpr-info.eu) (Source: gdpr-info.eu). China is absent from that list. Absent an adequacy decision, a data exporter must rely on Standard Contractual Clauses (SCCs), Binding Corporate Rules, or another Article 46 safeguard, and legal analysis of DeepSeek's hosted service found "we did not find a public enterprise DPA or AVV package for German procurement as of June 29, 2026," meaning the hosted product is "not procurement-ready in the way German legal and privacy teams usually require" (Source: compound.law). German state regulators have not softened their position: the Lower Saxony data protection authority "warned that, based on current knowledge, DeepSeek does not satisfy key requirements of the GDPR and the EU AI Act," and Berlin's Commissioner for Data Protection notified Apple and Google in mid-2025 that the DeepSeek app should be treated as illegal content because of unlawful transfers to China, with the June 2026 annual report noting the platforms rejected that takedown request and further Digital Services Act steps may follow (Source: compound.law) (Source: compound.law). Italy's Garante, which the reporting describes as "among the most proactive of the 31 data protection authorities in Europe on the use of AI," moved fastest, ordering DeepSeek blocked nationwide within roughly 72 hours of opening its inquiry after the company's answers were deemed "totally insufficient" (Source: reuters.com).

The US Bulk Data Transfer Rule. Executive Order 14117, implemented through a Department of Justice rule effective April 8, 2025, restricts transactions giving "countries of concern," a category that currently includes "China, Cuba, Iran, North Korea, Russia and Venezuela," access to bulk sensitive US personal data (Source: jacksonlewis.com). The rule's own worked example describes exactly the life sciences risk scenario: a chatbot trained on bulk sensitive personal health data that can "reproduce or otherwise disclose" that training data when prompted, licensed to a covered

person, which the DOJ classifies as a prohibited data brokerage transaction (Source: jacksonlewis.com). The specific bulk thresholds matter for life sciences data: "personal health data" triggers restrictions above 10,000 US persons, while human genomic data triggers restrictions above just 100 persons and other "omic" data above 1,000 persons (Source: jacksonlewis.com) (Source: jacksonlewis.com), thresholds that typical Phase 2 or 3 clinical trial datasets, patient support programs, or real-world evidence platforms can cross without difficulty. Penalties are severe: civil penalties up to "the greater of $368,136 or an amount that is twice the amount of the transaction," and willful violations can carry fines up to $1,000,000 and up to 20 years imprisonment for individuals (Source: jacksonlewis.com) (Source: jacksonlewis.com).

China's own cross-border transfer regime, and why it can cut in favor of self-hosting. China's data governance stack, the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL), treats health and genomic data as both a strategic economic resource and a national security asset (Source: atlanticcouncil.org). A 2025 Cyberspace Administration of China (CAC) FAQ clarified that outbound transfers of "important data" and personal information require one of three mechanisms: a CAC Security Assessment, Personal Information Protection Certification, or a filed Standard Contract, and confirmed that of 298 Security Assessment submissions reviewed as of March 2025, 44 involved important data and seven of those failed review (Source: arnoldporter.com). Notably for life sciences MNCs operating in China, the Beijing Free Trade Zone published a "negative list" in August 2024 that specifically names "the automobile and life sciences industries" as sectors eligible for streamlined, lower-friction cross-border data transfer within that zone (Source: arnoldporter.com), and multinational corporations with several Chinese subsidiaries may now submit a single Security Assessment or Standard Contract filing on behalf of all related entities (Source: arnoldporter.com). The Atlantic Council's analysis of this system concludes that it is "relatively open where data use advances state-backed innovation, clinical research, pharmaceutical development, and AI industrial policy," but closed wherever data mobility threatens state visibility, meaning the practical default recommendation for multinationals is to "assume localization for many categories of sensitive health and AI-training data" (Source: atlanticcouncil.org), and that the overall system "incentivizes a 'China-for-China' health AI architecture" (Source: atlanticcouncil.org).

Table 2 below summarizes how the major frameworks apply specifically to hosted Chinese AI model use as of July 2026.

FRAMEWORK	JURISDICTION	KEY REQUIREMENT OR THRESHOLD	STATUS FOR HOSTED CHINESE CHATBOTS/APIS
GDPR Article 44-49	European Union	Adequacy decision or Article 46 safeguard (SCCs, BCRs) required for any transfer outside the adequacy list	China not on the adequacy list (Source: gdpr-info.eu); no public DPA/SCC package found for DeepSeek's hosted service (Source: compound.law); Italy blocked DeepSeek nationally (Source: reuters.com)
US Bulk Data Transfer Rule (EO 14117)	United States	Personal health data above the >10,000-US-person threshold is covered when a country of concern or covered person receives access through a covered data transaction; data brokerage is prohibited, while vendor, employment, and investment agreements are restricted (Source: jacksonlewis.com)	Effective since April 8, 2025 (Source: jacksonlewis.com); civil penalties up to the greater of $368,136 or 2x the transaction value (Source: jacksonlewis.com)
China PIPL / DSL / CSL	China (outbound side)	Security Assessment, PIP Certification, or SCC Filing required for "important data" or bulk personal information exports	Beijing FTZ negative list exempts life sciences data from some restrictions within the zone (Source: arnoldporter.com); default posture is localization (Source: atlanticcouncil.org)
EU AI Act (Regulation (EU) 2024/1689)	European Union	High-risk classification for AI embedded in or acting as a medical device safety component	Fully applicable from August 2, 2026, with GPAI transparency obligations already in force since August 2025 (Source: digital-strategy.ec.europa.eu)

Reading Table 2 alongside Table 1 makes the practical guidance clear: a hosted service may require GDPR transfer safeguards and may warrant review under the US Data Security Program, depending on the data flow, entities, transaction type, and applicable thresholds. China's own export regime can also affect multinational processing arrangements. Self-hosting on a company's EU or US infrastructure may reduce or avoid a transfer to

the model developer where the architecture creates no such flow, but it does not eliminate analysis of the full deployment, applicable contracts, healthcare roles, security, validation, or bias considerations. Deployment approval should be based on a documented, jurisdiction-specific legal and technical review (US Department of Justice.

Life Sciences-Specific Compliance Obligations

Beyond generic data protection law, life sciences companies face a compliance layer specific to regulated drug, biologic, and device development that applies regardless of which AI model, Chinese or otherwise, is used.

HIPAA and the Business Associate Agreement gap. Any AI vendor that creates, stores, or transmits protected health information (PHI) on behalf of a covered entity must sign a Business Associate Agreement (BAA) under HIPAA. As one industry analysis of the broader shadow-AI problem in pharma put it, "HIPAA demands comprehensive audit trails for all electronic protected health information (ePHI) access, yet companies cannot track what flows into shadow AI tools," and "21 CFR Part 11 applies to electronic records required by applicable FDA predicate rules or submitted to FDA; its validation and electronic-signature requirements depend on the regulated records and how they are used" (Source: contractpharma.com). Neither DeepSeek nor Kimi's consumer-facing services offer a public BAA, and their privacy policies are written for general consumers, not regulated healthcare data processors. Separately, HHS's Office for Civil Rights has issued a "Dear Colleague" letter confirming it will enforce Section 1557 nondiscrimination protections against AI-based patient care decision support tools effective from July 5, 2024, with a broader duty to identify and mitigate discrimination risk from such tools effective May 1, 2025 (Source: reedsmith.com). Any Chinese model used in a patient-facing or clinical decision context inherits this obligation identically to any other AI system.

FDA's AI credibility framework. FDA's January 2025 draft guidance, "Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products," applies to "the use of artificial intelligence (AI) to produce information or data intended to support regulatory decision-making regarding safety, effectiveness, or quality for drugs," and it establishes "a risk-based credibility assessment framework that may be used for establishing and evaluating the credibility of an AI model for a particular context of use" (Source: fda.gov). This applies with equal force to any Chinese open-weight model used to generate or analyze data supporting a regulatory submission; the model's country of origin does not change the credibility assessment obligation, but the opacity of the model's training data and post-training alignment (discussed further below) makes documenting that credibility harder for models like DeepSeek, whose developer has not publicly disclosed the post-training methodology behind its documented pro-state response bias.

GxP validation and GAMP 5. IntuitionLabs' own due diligence guidance for pharmaceutical AI buyers notes that "AI tools in pharma often fall under regulations (e.g. FDA, EMA, GxP, HIPAA)" and that buyers should verify vendors follow "FDA's AI/ML draft frameworks, GAMP 5, and ISO standards for medical devices and software," with "audit trails, validation documents, and risk assessments" treated as critical deliverables regardless of the model's provenance (Source: intuitionlabs.ai). The same guidance stresses that "contracts must explicitly restrict vendor reuse of sensitive prompts" for any generative AI system a pharmaceutical company adopts (Source: intuitionlabs.ai), a clause that is straightforward to negotiate with a Western vendor but effectively unobtainable with DeepSeek's hosted consumer service, whose privacy policy reserves broad rights to use input data for model training with only a narrow opt-out mechanism.

The EU AI Act's high-risk classification. Under Article 6 of the AI Act, "AI systems of the types listed in Annex III are always considered high-risk, unless they don't pose a significant risk to people's health, safety, or rights" (Source: artificialintelligenceact.eu), a category that includes AI safety components of medical devices. The Act "entered into force on 1 August 2024, and will be fully applicable 2 years later on 2 August 2026," with general-purpose AI model obligations, the category most Chinese foundation models fall into, already applicable since August 2, 2025 (Source: digital-strategy.ec.europa.eu) (Source: digital-strategy.ec.europa.eu). A political agreement reached May 7, 2026 delayed some high-risk system rules, but the GPAI transparency, copyright, and systemic-risk assessment obligations that apply to any large foundation model, including DeepSeek, Kimi, or Qwen, remain in force and were not part of that delay (Source: digital-strategy.ec.europa.eu).

Security, Censorship, and Model-Integrity Risk

Beyond data privacy law, life sciences organizations must weigh documented technical security and content-integrity findings that are independent of jurisdiction and go to whether a model can be trusted at all in a clinical or regulatory context.

NIST's Center for AI Standards and Innovation (CAISI) published a formal comparative evaluation in September 2025 that tested three DeepSeek models against four US models across 19 benchmarks. The results were unambiguous on security: "DeepSeek's most secure model (R1-0528) responded to 94% of overtly malicious requests when a common jailbreaking technique was used, compared with 8% of requests for U.S. reference models" (Source: nist.gov). In agentic settings, which matter directly to life sciences workflows that increasingly chain AI models to internal databases and tools, "agents based on DeepSeek's most secure model...were, on average, 12 times more likely than evaluated U.S. frontier models to follow malicious instructions designed to derail them from user tasks," with hijacked agents observed sending phishing emails, downloading malware, and

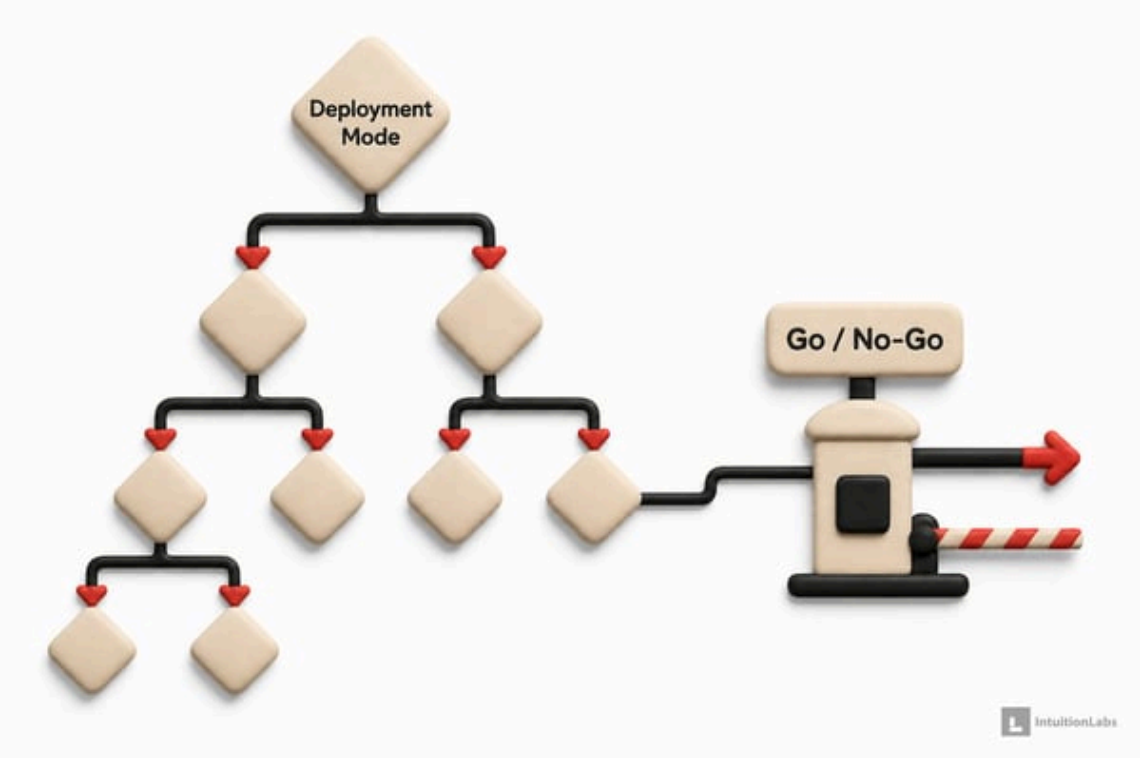
exfiltrating login credentials in CAISI's simulated environment (Source: nist.gov). CAISI also found DeepSeek models "advance Chinese Communist Party (CCP) narratives," echoing "four times as many inaccurate and misleading CCP narratives as U.S. reference models" (Source: nist.gov), a bias with direct clinical relevance given documented instances of the model providing state-favorable rather than medically accurate framing of public health policy questions. On raw capability, CAISI found "the best U.S. model outperforms the best DeepSeek model (DeepSeek V3.1) across almost every benchmark," with the largest capability gap in software engineering and cybersecurity tasks, and found that a US reference model was "35% less" expensive on average to reach comparable performance (Source: nist.gov), a finding that undercuts the pure cost-savings argument frequently cited by proponents of DeepSeek adoption. Adoption, meanwhile, has surged regardless of these findings: CAISI documented that "downloads of DeepSeek models on model-sharing platforms have increased nearly 1,000% since January 2025" (Source: nist.gov).

A peer-reviewed analysis published in *AI Ethics* examined this censorship pattern directly in a healthcare context, concluding that "the pro-state alignment of DeepSeek weakens the rationale for widespread adoption in sensitive domains involving vulnerable populations, particularly healthcare" (Source: pmc.ncbi.nlm.nih.gov), noting that the government's own evaluation body, CAISI, "found that DeepSeek poses security and censorship risks" independently (Source: pmc.ncbi.nlm.nih.gov). The same study documented that DeepSeek models have been downloaded "over 10 million times from the HuggingFace NLP platform" and that the DeepSeek chatbot recorded "over 57 million downloads from the Apple and Google app stores (based on data from May 2025)" (Source: pmc.ncbi.nlm.nih.gov) (Source: pmc.ncbi.nlm.nih.gov), underscoring that the scale of exposure is already enormous even as compliance and safety findings mount. Adding a national security dimension, a senior US State Department official told Reuters that "DeepSeek has willingly provided and will likely continue to provide support to China's military and intelligence operations," alleging the company is "sharing user information and statistics with Beijing's surveillance apparatus" and noting the company is "referenced more than 150 times in procurement records for China's People's Liberation Army" (Source: reuters.com) (Source: reuters.com) (Source: reuters.com). Reuters could not independently verify the procurement-record allegation, and DeepSeek did not respond to questions about its privacy practices, but the allegation itself, from a named government office, is a material fact for any life sciences risk committee weighing vendor concentration and geopolitical exposure.

The broader NIST AI Risk Management Framework's Generative AI Profile, published before the DeepSeek episode but directly applicable to it, identifies "data privacy" as one of "12 primary risks that are unique to, or exacerbated by, GenAI," alongside "information security" risks such as data poisoning and prompt injection, and "value chain and component integration" risk arising from "integration of nontransparent or third-party components" (Source: dlapiper.com) (Source: dlapiper.com) (Source: dlapiper.com). This framework applies equally to Chinese and Western models, but the CAISI and PMC findings above suggest the risks it describes are materially more acute for hosted Chinese models than for comparably-scaled Western alternatives.

A Risk-Based Framework for Evaluating Chinese AI Models in Life Sciences

Given the deployment-mode taxonomy, regulatory stack, and security findings above, life sciences AI governance committees need a structured way to translate these facts into a go/no-go decision for a specific proposed use case. IntuitionLabs' pharmaceutical AI vendor due diligence framework emphasizes that "pharmaceutical buyers must conduct rigorous due diligence to validate AI vendor claims before signing contracts or deploying solutions" (Source: intuitionlabs.ai), and that same discipline applies with particular force to Chinese model evaluation, where the vendor relationship, data flows, and jurisdictional exposure differ substantially from a typical US or European AI vendor engagement.



A practical decision framework should walk through the following questions in order:

- **What is the deployment mode?** Hosted consumer app, vendor API, or fully self-hosted open-weight deployment. This single variable, as established above, determines nearly everything else.
- **What data classes will touch the model?** Anonymized literature search and general knowledge-work carry materially lower risk than clinical trial data, patient records, or unpublished molecular structures, which trigger HIPAA, GDPR special-category data rules, and the Bulk Data Transfer Rule's health-data threshold simultaneously.
- **Does the deployment cross a regulated jurisdiction boundary?** Self-hosting DeepSeek or Kimi weights entirely within a single company's EU-region cloud tenancy, with no calls back to the original developer's infrastructure, avoids the GDPR third-country transfer analysis and the Bulk Data Rule's cross-border test, provided the underlying infrastructure provider itself is properly contracted.
- **Can the vendor (or, for open-weight models, the deployment) support a signed Business Associate Agreement, Data Processing Agreement, or equivalent, and provide audit-trail and validation documentation consistent with GAMP 5 and 21 CFR Part 11?** Hosted DeepSeek and Kimi consumer services generally cannot; a self-hosted deployment inherits whatever contractual and validation posture the deploying organization builds around it.
- **Is the use case one where documented censorship or pro-state bias in model outputs creates clinical or regulatory risk?** Any use case touching public health policy framing, comparative government response analysis, or politically sensitive epidemiological topics should be treated as high-risk for DeepSeek specifically, per the PMC and CAISI findings above.
- **Has the model been evaluated under the FDA's AI credibility framework for its specific context of use**, with documented data provenance, performance metrics, and bias testing, regardless of whether the model is American, European, or Chinese in origin?

Table 3 below applies this framework to summarize residual risk by deployment mode for a representative set of life sciences use cases.

DEPLOYMENT MODE	DATA RESIDENCY OUTCOME	GDPR / BULK DATA RULE EXPOSURE	REPRESENTATIVE SUITABLE USE CASE	RESIDUAL RISK
Hosted consumer chatbot (deepseek.com, kimi.com)	PRC (DeepSeek) or Singapore (Kimi), outside company control	High: no adequacy decision, no public DPA/BAA, thresholds easily crossed	Public, non-sensitive literature scanning with no proprietary or patient data	High; several jurisdictions already restrict or ban this mode
Vendor-hosted API	Vendor-controlled infrastructure; the applicable jurisdictions depend on the parties and data flow	Moderate to high, depending on contract terms, transfer safeguards, transaction type, and whether a DPA is available	Prototype evaluation with fully synthetic or public test data only	Moderate to high; requires case-by-case legal and contractual review
Self-hosted open-weight deployment	Entirely within the company's own controlled infrastructure and jurisdiction	Low for cross-border transfer specifically; standard AI governance obligations still apply	Internal drafting assistance, code generation, and literature summarization on de-identified data, subject to full GxP validation	Low to moderate; security, bias, and validation review still required

The table underscores that self-hosting is not a compliance shortcut, it is a prerequisite that then still requires the full complement of GxP validation, security testing, and bias review any AI system would need in a regulated life sciences environment. It converts an unanswerable cross-border legal question into a manageable, standard AI governance exercise.

Data Analysis and Evidence

The quantitative picture underlying this analysis spans adoption, cost, security, and enforcement data. On adoption, DeepSeek models saw downloads increase "nearly 1,000% since January 2025" on model-sharing platforms according to NIST CAISI's evaluation (Source: nist.gov), while independent peer-reviewed tracking found over 10 million HuggingFace downloads and over 57 million app store downloads by May 2025 (Source: pmc.ncbi.nlm.nih.gov) (Source: pmc.ncbi.nlm.nih.gov). On the Kimi side, Moonshot AI's valuation climbed to over $20 billion on roughly $2 billion in fresh funding, with annual recurring revenue surpassing $200 million as of April 2026 (Source: forbes.com) (Source: forbes.com), evidence of how quickly the commercial footprint of these models is scaling even as regulatory scrutiny intensifies in parallel.

On cost, K2's API pricing of roughly $0.15 per million input tokens and $2.50 per million output tokens undercuts incumbent Western frontier providers by an order of magnitude on list price (Source: intuitionlabs.ai), yet CAISI's independent benchmark testing found that when accounting for the number of tokens needed to reach equivalent task performance, "one U.S. reference model costs 35% less on average than the best DeepSeek model to perform at a similar level" (Source: nist.gov), a reminder that headline per-token pricing does not capture total cost of achieving a given output quality.

On security, the gap CAISI documented is large by any standard: a 94% jailbreak success rate against DeepSeek's most secure model compared with 8% for US reference models is not a marginal difference, it represents roughly a twelvefold difference in exploitability, consistent with the separately reported twelvefold increase in malicious-instruction compliance for DeepSeek-based autonomous agents (Source: nist.gov) (Source: nist.gov).

On regulatory enforcement velocity, the pace of formal actions against DeepSeek specifically is instructive: Texas issued the first US state-level ban on January 31, 2025, with Governor Greg Abbott stating that "Texas will not allow the Chinese Communist Party to infiltrate" the state's critical infrastructure through what he called data-harvesting AI (Source: insidegovernmentcontracts.com), Italy's Garante moved from opening an inquiry to a national block within roughly 72 hours in January 2025 (Source: reuters.com), the US Bulk Data Transfer Rule went from an executive order to an enforceable rule with a defined grace period in roughly fourteen months (Source: jacksonlewis.com), and German state authorities have continued escalating through mid-2026, with the Berlin DPA's most recent annual report signaling further Digital Services Act steps are still to come (Source: compound.law). This is not a settled, static compliance picture; it is an actively escalating one, which itself is a data point life sciences risk committees should weigh heavily given the multi-year timelines typical of drug development and clinical trial programs.

Separately, the general (not China-specific) state of AI data governance in pharma provides useful baseline context: the Kiteworks-sponsored survey of 461 cybersecurity, IT, risk, and compliance professionals found only 17% of organizations, across the life sciences and adjacent sectors, have automated controls preventing sensitive data leakage into any AI tool, with 40% relying only on employee training, 20% on unverified warning emails, 10% on guidelines alone, and 13% having no policy whatsoever (Source: contractpharma.com). Federal AI-related regulatory activity has also accelerated sharply, with US federal agencies issuing 59 AI-related regulations in 2024, more than double the 25 issued in 2023 (Source: contractpharma.com), a trajectory that suggests the compliance burden facing any AI vendor selection, Chinese or otherwise, will only grow more demanding through the remainder of this decade.

Case Studies and Real-World Examples

Italy's national block of DeepSeek (January 2025). Italy's Garante ordered DeepSeek's chatbot blocked nationally after the company failed to adequately answer questions about "what personal data is collected, from which sources, for what purposes, on what legal basis and whether it is stored in China" (Source: reuters.com). DeepSeek's response reportedly argued it "should not be subject to local regulation or the jurisdiction of the Garante," a position the regulator's board member called counterproductive: "Not only did DeepSeek's response not give us any reassurance, it worsened their position, and that's the reason we decided to order the block" (Source: reuters.com). This case is directly instructive for any European life sciences subsidiary considering the hosted service: a national regulator can and did suspend access with immediate effect, and Ireland and France opened parallel inquiries around the same time (Source: reuters.com).

A wave of US state and federal device bans (January to February 2025). Texas became the first US state to act, with Governor Greg Abbott issuing a ban on China-affiliated AI applications, including DeepSeek, on state government-issued devices on January 31, 2025 (Source: insidegovernmentcontracts.com), stating that "Texas will not allow the Chinese Communist Party to infiltrate" the state's critical infrastructure through data-harvesting AI (Source: insidegovernmentcontracts.com). New York followed on February 10, and "on February 11, Virginia became the third state to prohibit DeepSeek on government devices with Governor Glenn Youngkin's signing of Executive Order 46" (Source: insidegovernmentcontracts.com), an order that, per Virginia's own university compliance notice, prohibits "the use of DeepSeek on any state or university issued, owned or leased equipment" (Source: jmu.edu). At the federal level, the Defense Information Systems Agency "began blocking access to DeepSeek on the Pentagon's IT networks on January 28" (Source: insidegovernmentcontracts.com), while NASA's Chief AI Officer separately barred personnel from using DeepSeek "with NASA's data and information or on government-issued devices and networks" (Source: insidegovernmentcontracts.com). This case matters for any life sciences company with government contracts, academic medical center affiliations, or public university research partnerships, all of which increasingly fall under similar device-level restrictions.

Congressional legislative response. Beyond executive and agency action, Representative Josh Gottheimer introduced the "No DeepSeek on Government Devices Act" (H.R. 1121) in February 2025, which "directs the Office of Management and Budget to develop standards and guidance requiring removal of the DeepSeek application from federal agency information technology," extending to "any successor application developed or provided by High-Flyer," DeepSeek's parent hedge fund, "or entities owned by High-Flyer" (Source: congress.gov). While this bill remains at the introduced stage as of this writing, it signals sustained bipartisan legislative interest in formalizing what is currently a patchwork of executive and agency-level restrictions.

Beijing hospital deployment and the medical research community's own caution (2025). Inside China, the adoption pattern cuts the other way: as of early 2025, at least 300 hospitals in China had started using DeepSeek's large language models in clinical diagnostics and medical decision support (Source: scmp.com), prompting a peer-reviewed commentary in *Nature Medicine* warning of a regulatory "gray area" and documenting "a real-world system architecture of DeepSeek OPD at Hospital P in Beijing" as a case study in rapid, under-governed clinical deployment (Source: preview-www.nature.com). Even within China, where the model faces none of the cross-border restrictions discussed above, a team of medical researchers publishing in *JAMA* warned that DeepSeek's tendency to generate "plausible but factually incorrect outputs" could lead to "substantial clinical risk" despite its strong reasoning capabilities (Source: scmp.com), a useful reminder that the compliance concerns raised in this report are not solely a function of Western regulatory friction but reflect genuine, model-level clinical governance gaps.

The Beijing Free Trade Zone life sciences carve-out (August 2024, clarified June 2025). In a rare example of a Chinese regulatory action easing rather than tightening cross-border data flow, the Beijing FTZ's negative list "covers, among other sectors, the automobile and life sciences industries," meaning multinational life sciences companies operating within that specific zone benefit from streamlined data export rules relative to the general PIPL regime (Source: arnoldporter.com). The Cyberspace Administration of China's April 2025 FAQ confirmed that negative lists from one FTZ "will be automatically effective in other FTZs to ensure consistency across regions" (Source: arnoldporter.com), giving multinational pharmaceutical companies operating in China a concrete, if narrow, pathway for lower-friction data movement that is directly relevant to any China-based R&D operation considering domestic AI tool adoption for local clinical trial support.

Implications and Future Directions

The regulatory trajectory across all three major jurisdictions points toward tightening rather than loosening restrictions on hosted Chinese AI model use in regulated data contexts, even as the underlying models continue to advance technically. Kimi K3's July 2026 launch, at 2.8 trillion parameters and explicitly marketed as a "direct challenger to leading systems offered by Anthropic and OpenAI" (Source: forbes.com), demonstrates that Chinese labs are closing rather than widening the capability gap despite continued US export controls on advanced AI chips, with Bank of America analysts noting in a research note that Moonshot "has demonstrated it can make major advancements by improving how it trains and designs its models" even with limited access to the most advanced hardware (Source: forbes.com). This means life sciences procurement pressure to evaluate these models will intensify, not fade, making a durable governance framework more valuable than a one-time ban-or-allow decision.

On the EU side, the AI Act's full applicability from August 2, 2026 will bring general-purpose AI transparency and systemic-risk obligations to bear on any large Chinese foundation model marketed or used within the Union, while the parallel "AI omnibus" simplification package, politically agreed May 7, 2026, defers some high-risk system rules to December 2027 without touching the GPAI obligations already in force (Source: digital-strategy.ec.europa.eu). On the US side, the Bulk Data Transfer Rule's enforcement posture will mature past its initial grace periods, and CAISI's mandate under the America's AI Action Plan to continue evaluating "capabilities of U.S. and adversary AI systems" and "potential security vulnerabilities and malign foreign influence" suggests further formal government assessments of newer Chinese models, including Kimi K3 and updated DeepSeek releases, should be expected within the next reporting cycle (Source: nist.gov).

Within China itself, the Atlantic Council's analysis anticipates a "near-term" horizon of "refinement, selective easing, and controlled facilitation," a "medium-term" shift toward "differentiation, institutionalization, and post-transfer oversight," and a "long-term" settlement into "managed openness within a sovereignty-centered system" (Source: atlanticcouncil.org) (Source: atlanticcouncil.org), a trajectory that suggests the Beijing FTZ-style carve-outs for life sciences data may expand to additional zones and sectors even as the default posture toward foreign AI model access to Chinese-sourced health data remains restrictive. For life sciences companies with both Western compliance obligations and Chinese R&D or manufacturing operations, this points toward an increasingly bifurcated technology stack: domestically-hosted, China-approved AI tools for China-based operations, and separately governed, self-hosted or Western-vendor AI tools for global and Western-market operations, rather than a single unified AI vendor strategy spanning both environments.

Frequently Asked Questions (FAQs)

Is DeepSeek safe for pharmaceutical companies? The hosted consumer app and API are not appropriate for any workflow involving patient data, unpublished clinical results, or proprietary molecular structures, given the company's own privacy policy confirms PRC data storage (Source: cdn.deepseek.com), the absence of GDPR adequacy for China (Source: gdpr-info.eu), and NIST CAISI's documented security and censorship shortcomings (Source: nist.gov). Self-hosted deployment of the open-weight DeepSeek models on the company's own controlled infrastructure presents a substantially different, and more defensible, risk profile, subject to standard GxP validation.

Can pharma companies use DeepSeek or Kimi? A self-hosted open-weight deployment may be evaluated with appropriate GxP validation, security review, data-governance controls, and confirmation that no data flows to the developer. A hosted consumer app or vendor API requires a case-specific assessment of the actual data flow, entity status and healthcare role, contract terms, transfer safeguards, and whether the Data Security Program covers the transaction; it is not subject to a universal China-service ban. Regulated personal, health, or genomic data warrants heightened review and deployment approval from qualified counsel and compliance teams (US Department of Justice; HHS.

Is Kimi K3 data sovereignty compliant? Kimi's developer, Moonshot AI, stores hosted API data in Singapore rather than mainland China, per its own OpenPlatform privacy policy (Source: platform.kimi.ai), which is a materially different posture than DeepSeek's explicit PRC storage. However, Singapore is outside the EU adequacy list, so GDPR-covered transfers still require an applicable transfer mechanism and safeguards. As of July 26, 2026, K3 weights were pending, so it should not be described as a self-hosted open-weight deployment; K2 is the Moonshot model described here as released under the Modified MIT License (Kimi K3 preview; Kimi K2 repository.

Does the GDPR permit using Chinese AI models at all? Only if a valid transfer mechanism is in place, an adequacy decision (China has none), Standard Contractual Clauses, Binding Corporate Rules, or explicit informed consent for a specific, non-repetitive transfer (Source: gdpr-info.eu). In practice, no public SCC or DPA package has been identified for DeepSeek's hosted consumer service as of mid-2026 (Source: compound.law), making GDPR compliance for the hosted service effectively unachievable for personal data workflows.

What data sovereignty requirements apply to AI in healthcare specifically? Beyond general GDPR and PIPL transfer rules, HIPAA requires a Business Associate Agreement for any vendor touching protected health information, FDA's 21 CFR Part 11 applies when electronic records are created, modified, maintained, archived, retrieved, transmitted, or submitted under applicable FDA predicate-rule requirements; FDA's scope guidance also describes specified enforcement discretion (FDA, and the US Bulk Data Transfer Rule imposes a specific 10,000-person threshold for personal health data transactions with countries of concern (Source: jacksonlewis.com).

Are open-source Chinese AI models a bigger or smaller regulatory risk than closed hosted models? A genuinely self-hosted deployment can reduce cross-border data-transfer exposure when no operational data is returned to the original developer, but the license must be reviewed model by model. For DeepSeek-V3, the code is MIT-licensed while the weights are governed by a separate Model License with use-based restrictions and other conditions; Kimi K2 uses a Modified MIT License, and Qwen licensing varies by model (DeepSeek-V3 repository; DeepSeek Model License; Kimi K2 repository; Qwen repository. The residual risk shifts from data sovereignty law to standard AI governance concerns: model bias, security vulnerabilities baked into the weights themselves, and validation documentation, all of which require the same due diligence IntuitionLabs recommends for any AI vendor evaluation in a regulated pharmaceutical environment (Source: intuitionlabs.ai).

How should a life sciences company structure AI vendor due diligence for a Chinese model? The same multidisciplinary framework used for any AI vendor, technical validation of data provenance and performance, regulatory and compliance assessment against FDA, EMA, GxP, and HIPAA requirements, security assessment of the deployment architecture, and contractual review to ensure sensitive prompts cannot be reused for vendor-side model training (Source: intuitionlabs.ai), applied with heightened scrutiny given the documented censorship and security findings specific to at least one major Chinese model family.

Conclusion

Life sciences companies asking whether they can use Chinese AI models are, in most cases, asking the wrong question in isolation. The country of origin of a model is a proxy for a set of underlying risks, data residency, cross-border transfer law, vendor contractual posture, and documented security and bias characteristics, and each of those underlying risks varies dramatically depending on deployment mode rather than developer nationality alone. A hosted DeepSeek chatbot processing patient data is nearly impossible to reconcile with GDPR, carries meaningful exposure under the US Bulk Data Transfer Rule once clinical dataset thresholds are crossed, and has already been formally restricted by multiple governments and flagged by the United States' own standards body for documented security and censorship shortcomings. The same underlying model, self-hosted on a life sciences company's own controlled infrastructure with no data returned to its developer, presents a fundamentally different and more manageable risk profile, one that converts an unresolvable cross-border legal question into the same GxP validation, security review, and vendor governance exercise any AI deployment requires in a regulated environment.

This distinction will only grow more consequential as Chinese labs continue to close the capability gap, evidenced by Kimi K3's July 2026 launch at 2.8 trillion parameters, and as regulatory regimes in the EU, the United States, and China itself continue to mature and, in most respects, tighten. Life sciences organizations should treat this as an ongoing governance discipline rather than a one-time policy decision: establish a clear deployment-mode classification for any proposed AI tool, map the specific data classes involved against HIPAA, GDPR, and Bulk Data Transfer Rule thresholds, insist on the same contractual and validation documentation required of any AI vendor regardless of national origin, and revisit the assessment as both the underlying models and the surrounding regulatory frameworks continue to evolve. Organizations that build this discipline now will be positioned to capture the genuine cost and capability advantages these models offer without inheriting the compliance and security liabilities that have already triggered national bans, formal government investigations, and documented security failures across the first eighteen months of the Chinese open-weight AI era.

Tags: chinese ai models, deepseek, kimi k2, kimi k3, data sovereignty, gdpr compliance, pharma ai compliance, ai vendor due diligence, life sciences ai, data privacy regulations

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.

Leading Claude & ChatGPT AI Enablement and Training: Help biotech and pharmaceutical teams adopt Claude and ChatGPT through practical training, governed workflows, use-case development, and implementation designed for regulated environments.

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 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.

© 2026 IntuitionLabs.ai. All rights reserved.