IntuitionLabs

INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

CIOMS XIV Implementation: Deploying AI in Pharmacovigilance

> Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2026-04-04 · cioms xiv · ai in pharmacovigilance · ai governance · machine learning · safety monitoring · algorithm validation · pv automation · adverse event reporting

Original article: https://intuitionlabs.ai/articles/cioms-xiv-ai-pharmacovigilance-implementation



In this article

1. Executive Summary
2. Introduction and Background
3. The CIOMS Working Group XIV Framework
4. CIOMS and Its Mandate
5. Implementing AI in PV: An Operational Playbook
6. AI Use-Cases in Pharmacovigilance (Table 1)
7. Data Management and Quality
8. Model Development and Validation
9. Human Oversight and Workforce
10. Validation, Testing, and Continuous Monitoring
11. Transparency and Explainability
12. Ethical and Fairness Considerations
13. CIOMS Guiding Principles vs Implementation Steps (Table 2)
14. Implementation Steps and Best Practices
15. Case Studies and Real-World Examples
16. Discussion: Implications and Future Directions
17. Data and Evidence Synthesis
18. Conclusion

Executive Summary

The convergence of **artificial intelligence (AI)** with **pharmacovigilance (PV)** has emerged as a critical priority for the pharmaceutical industry and regulators. In recent years, the volume and complexity of PV data (spontaneous reports, clinical studies, medical literature, social media, etc.) have grown exponentially, straining traditional safety monitoring systems (edit.uppsalareports.org) (oboe.com). For historical context, UMC reported that **VigiBase** reached 28 million reports in 2021, after adding approximately 2 million reports in the four months following May 2021 (Uppsala Reports). Likewise, major regulatory reporting systems such as FDA's Adverse Event Monitoring System (AEMS), formerly FAERS handle millions of reports annually (oboe.com). This **data avalanche** has motivated the PV community to explore AI and automation to improve efficiency and insight. Leading consultancies note that AI methods can "automate end-to-end post-launch PV" – from case intake and coding to real-time signal detection – thereby improving patient safety through faster detection of adverse events (www.deloitte.com) (oboe.com).

However, AI in PV also poses significant challenges. Unlike consumer applications, AI tools in PV have *"direct or indirect influence over patient safety,"* which calls for careful governance akin to medicinal products (cioms.ch). Recognizing this, the Council for International Organizations of Medical Sciences (CIOMS) established Working Group XIV to create global consensus guidance. In December 2025, CIOMS published its *"Artificial Intelligence in Pharmacovigilance"* report, providing a **principles-based implementation playbook**.

The CIOMS XIV report emphasizes seven core principles – including a risk-based approach, human oversight, validity and robustness, transparency, data privacy, fairness, and governance – and offers concrete recommendations for deploying AI safely (www.qualio.com).

This report reviews the **new CIOMS XIV framework** in detail and provides an **implementation playbook** for AI in PV. We begin with background on PV systems and the impetus for AI, then summarize the CIOMS recommendations. We next develop in-depth guidance on implementing AI under this new framework: covering data management, algorithm development and validation, human-machine collaboration, transparency and ethics, and ongoing governance (see **Table 2**). We illustrate with real-world examples (e.g. national regulator AI pilots, pilot studies of AI case processing (www.deloitte.com) (pmc.ncbi.nlm.nih.gov)), industry surveys, and case data. We also include tables summarizing common AI use-cases in PV and aligning CIOMS principles with concrete implementation steps. Finally, we discuss future implications, including regulatory trends (e.g. forthcoming AI legislation) and the evolving role of PV professionals. All claims are extensively sourced from CIOMS, industry publications, academic literature, and PV experts. This comprehensive playbook is intended to guide PV organizations through the safe and effective **deployment of AI under the CIOMS XIV framework**.

Introduction and Background

Pharmacovigilance (PV) – the science of detecting, assessing, and preventing adverse effects of medical products – is traditionally labor-intensive and manually driven. Each year, pharmaceutical companies and regulatory agencies worldwide process **millions** of safety reports (ICSRs) describing adverse drug reactions (ADRs). For example, some large pharmaceutical firms receive **up to one million ICSRs annually**, while Schmider et al., citing the 2016 PVNet benchmark, describe case processing as using **up to two-thirds of internal PV resources** (oboe.com) (pmc.ncbi.nlm.nih.gov). These ICSRs arrive from diverse sources (spontaneous reports, literature, patient programs, etc.) and in varying formats, many as free-text documents that must be coded and entered into databases. Systems such as FDA's Adverse Event Monitoring System (AEMS), formerly FAERS, and the WHO's VigiBase receive millions of reports and continue to grow rapidly (oboe.com) (edit.uppsalareports.org). For instance, UMC reported that VigiBase reached 28 million reports in **2021** during the COVID-19 vaccine reporting surge (Uppsala Reports). Global events (pandemics, large-scale vaccination drives) and digital health trends (social media, electronic health records) have accelerated PV data volumes, straining existing workflows.

AI in PV is already addressed in regulatory guidance. EMA's September 2024 reflection paper covers adverse-event report management and signal detection, and states that marketing authorisation holders remain responsible for validating, monitoring and documenting model performance (EMA, section 2.3.7). On 14 January 2026, EMA and FDA announced ten good-AI-practice principles covering the medicines lifecycle, including safety monitoring (EMA–FDA announcement). Further guidance is being developed. Assess AI-enabled PV systems against applicable legal requirements; CIOMS's consensus recommendations provide complementary guidance. The manpower challenge is acute: in-depth case processing (intake, coding, narrative review, etc.) may require extensive human effort. Schmider et al. (2019) documented that case processing can consume **up to two-thirds of a company's PV resources** (pmc.ncbi.nlm.nih.gov). Consequently, companies and regulators are keen to adopt automation to improve efficiency and consistency.

In recent years, **AI and machine learning (ML)** techniques have shown promise in automating PV tasks. Applications include natural-language processing (NLP) to extract information from narrative reports, automated coding of terms, duplicate-report detection, literature surveillance, and preliminary signal screening (www.deloitte.com). Pilot studies have demonstrated feasibility: an industry-led pilot trained ML algorithms using adverse-event source documents and corresponding safety-database fields as answer keys, without additional source-document annotation (Schmider et al.). The same study noted that applying AI "represents an opportunity to affect the strongest PV cost driver" (safety case processing) (pmc.ncbi.nlm.nih.gov). Digital health and AI have thus begun to "transform PV end-to-end," with promises of detecting new safety signals faster and freeing specialists to focus on complex analysis (www.deloitte.com) (pmc.ncbi.nlm.nih.gov).

However, PV professionals rightfully view AI with caution. Unlike other industries, errors in PV systems have *patient safety implications*. Automated decisions could miss rare but critical adverse events, or output erroneous alerts. PV involves sensitive personal data (often multi-country), raising data-privacy and ethical issues. Moreover, many AI techniques (especially advanced "Generative AI" models) are opaque by design. In short, AI in PV *cannot* be treated like a black-box cost-saver; it requires robust validation and oversight. As one industry expert notes, companies remain "highly interested" in ML/AI *not for automating simple tasks alone but for achieving human-like interpretation of data and decision-making*, which introduces novel challenges such as training data quality and lack of regulatory guidance (pmc.ncbi.nlm.nih.gov).

These concerns set the stage for international guidance. In May 2022, CIOMS launched Working Group XIV on AI in PV, convening experts from regulators, industry, and academia to define best practices. After broad consultation, the CIOMS WG XIV report was finalized on 4 December 2025 (cioms.ch). This report is the **first** authoritative, consensus-based framework for AI in PV. It treats AI systems **analogously to medical products** – just as drugs have approved indications and known side effects, AI tools must have defined use-cases, performance limits, and controls (cioms.ch). CIOMS does **not** prescribe specific AI technologies or use cases; rather, it establishes guiding principles and practical considerations to ensure AI is used *responsibly* in PV. According to CIOMS, AI in PV is "at the intersection of pharmacovigilance, computer science, regulation, law, medicine, human rights, psychology and social science," and must be governed accordingly (cioms.ch).

This report ("Implementing CIOMS XIV: A Playbook") provides an **in-depth guide** to deploying AI under the new CIOMS framework. We review the CIOMS recommendations (risk-based oversight, validation, transparency, etc.) and then translate them into actionable steps. We highlight multiple perspectives – regulatory, industry, technical, and ethical – using data, case examples, and literature. Readers will find sections on data requirements, model development, human–AI collaboration, validation metrics, transparency and ethics, governance structures, and future outlooks. The goal is to offer a **comprehensive roadmap** for PV professionals seeking to implement AI solutions in compliance with CIOMS XIV.

The CIOMS Working Group XIV Framework

CIOMS and Its Mandate

The Council for International Organizations of Medical Sciences (CIOMS) is a global body (affiliated with WHO and UNESCO) that traditionally issues consensus guidelines on drug safety and ethics (e.g. CIOMS Working Group VIII report on signal detection and Working Group IX on risk management (www.scribd.com) (cioms.ch)). CIOMS Working Group XIV was tasked with developing principles and guidance for artificial intelligence and intelligence augmentation in pharmacovigilance (CIOMS). The WG consisted of statisticians, computer scientists, regulators, ethicists, PV professionals, and patient-representatives. After collecting extensive feedback from industry and regulatory bodies worldwide, the group published its report in December 2025 (cioms.ch).

The **CIOMS XIV report** (formatted and available through CIOMS) is a **204-page document**, structured into chapters on introduction, landscape analysis, implementation considerations, and future outlooks. Importantly, it is *principles-based*, not a narrow checklist. As the report emphasizes: " [AI in PV] is a rapidly emerging cross-disciplinary field…(so) it is important to establish the approved indications, posology, side effects, and warnings and precautions for use of artificial intelligence in pharmacovigilance" (cioms.ch). In other words, PV organizations must treat AI tools with the same caution as medicinal products, defining precisely *how* and *when* each AI system should be applied, and documenting its known limitations (cioms.ch) (www.qualio.com).

Key Themes of the CIOMS Report

The CIOMS XIV report does **not** list specific AI algorithms or software to use. Instead, it lays down **guiding principles** that any AI deployment in PV should follow. The report identifies seven central principles (echoed by industry consensus surveys (pmc.ncbi.nlm.nih.gov)):

1. **Risk-Based Approach:** The level of oversight and validation should be proportional to the risk posed by the AI system (www.qualio.com). High-impact use-cases (e.g. systems influencing safety decisions, like automated signal prioritization) demand rigorous controls, whereas lower-risk tools (e.g. workflow efficiency bots) might require simpler review (www.qualio.com). CIOMS stresses that organizations should *classify* each AI application by its **safety-criticality** and document this risk assessment.
2. **Human Oversight:** AI systems must include defined human roles. CIOMS distinguishes *human-in-the-loop* systems (humans make final decisions) from *human-on-the-loop* systems (AI handles more while humans monitor) (www.qualio.com). Crucially, humans maintain accountability for all PV decisions. PV teams should plan for how roles will evolve (e.g. moving from manual to supervisory tasks) as AI is adopted (www.qualio.com).
3. **Validity & Robustness:** AI tools must be rigorously tested to ensure reliable performance in real-world PV settings (www.qualio.com). This includes using **representative test datasets** (covering all relevant data sources, patient subgroups, and product types) (www.qualio.com). Because PV deals with rare events (few reports for a given drug-event), CIOMS notes that evaluation sets may need artificial

enrichment (oversampling safety-signals) to adequately assess sensitivity (www.qualio.com). Performance metrics and validation protocols should be predefined, and tools must be stress-tested for corner cases (including adversarial scenarios).

4. **Transparency:** CIOMS calls for clear transparency about AI use. Stakeholders (PV staff, regulators, patients) should understand that AI systems are in use, what data they use, and what outputs they produce (www.qualio.com). The report recommends documenting each AI model's purpose, data sources, and known limitations in plain language. Methods of *explainability* (e.g. showing which features contributed to a decision) can help build trust, though CIOMS cautions that explainability techniques only provide *plausible* reasoning, not exact explanations (www.qualio.com).
5. **Data Privacy:** AI can introduce new privacy concerns, especially with unstructured health data and advanced models (e.g. large language models) (www.qualio.com) (www.scribd.com). CIOMS emphasizes "privacy-by-design": before deploying AI, perform data-protection impact assessments, apply encryption/anonymization where needed, and strictly govern any linkage of datasets (www.qualio.com). PV systems must remain adaptable to evolving data protection laws (e.g. GDPR, HIPAA, or local regulations). Special care is urged when using cloud-based or external AI services.
6. **Fairness & Equity:** The report addresses bias risk. AI can inadvertently disadvantage specific sub-populations (e.g. under-reporting for certain demographic groups). CIOMS advises ensuring training data **reflects the diversity** of the patient populations who will use the medicines (www.qualio.com). During validation, evaluate model performance across age, sex, ethnicity, geography, etc., to detect inequities. Gaps in reference data (like under-reporting in low-income regions) should be recognized, and mitigation strategies (e.g. targeted data collection, transfer learning) employed (www.qualio.com).
7. **Governance & Accountability:** The final principle is to govern AI across its lifecycle. CIOMS insists on clear ownership ("who is responsible for which AI system") and thorough documentation (www.qualio.com). This includes version-control of models and data, audit trails of decisions, and ongoing monitoring of AI performance. Roles and responsibilities must be explicitly defined (data science team, PV reviewers, quality assurance, etc.) to ensure accountability (www.qualio.com). Importantly, governance frameworks should **evolve** as technologies and regulations change (www.qualio.com).

Together, these principles form a **framework** rather than a step-by-step recipe. Table 2 (below) summarizes each principle and suggested implementation actions. In the following sections, we dive deeply into how to operationalize these principles in practice, illustrating with examples and data where possible.

Implementing AI in PV: An Operational Playbook

Below we translate the CIOMS principles into actionable steps and considerations for PV organizations. We begin by surveying common **use-cases and AI methods** in PV (Table 1), then discuss each key domain: data management, model development and validation, human oversight, transparency, privacy, fairness, and governance. We reference both CIOMS guidance and real-world evidence.

AI Use-Cases in Pharmacovigilance (Table 1)

AI and automation can be applied across many PV processes. **Table 1** lists representative use-cases, example tasks, AI techniques, and CIOMS considerations for each. Many of these are already in pilot or production (even if not fully replacing humans). For instance, “Case Intake” (the first step of receiving and logging reports) can be automated with **Robotic Process Automation (RPA)** and **Optical Character Recognition (OCR)** to digitize incoming forms, while NLP extracts key fields automatically (oboe.com). “Medical Coding and Data Extraction” uses NLP/ML to assign MedDRA terms and pull out age, dose, etc. CIOMS emphasizes data quality in these steps: human review is still needed to ensure accuracy, and any AI flags for low-confidence should trigger manual check.

Other use-cases include **duplicate detection** (clustering similar reports via text-similarity algorithms), **signal detection** (machine learning models scanning real-time data for unusual drug-event patterns), and **literature and social media monitoring** (text mining publications and posts to flag potential ADRs). Emerging applications involve **large language models (LLMs)** for summarizing narratives or drafting initial case assessments – though CIOMS cautions that generative AI systems require *particular oversight* due to risks like “hallucinations” (www.scribd.com). The “Triage & Prioritization” use-case refers to algorithms that rank cases by seriousness for human review. Each implementation carries benefits (efficiency, speed) but also risks (data bias, errors). For every application, one must apply CIOMS’s risk-based mindset: highly automated systems handling critical decisions need heavier validation and oversight (www.qualio.com).

Table 1: Examples of AI Applications in Pharmacovigilance *(Adapted from CIOMS and industry sources)*

PV Process	Example Tasks	AI/Techniques	CIOMS Considerations	Benefits/Evidence
Case Intake Automation	- Digitizing emailed/faxed reports - Extracting structured fields (patient, drug, event)	OCR, RPA, simple NLP	Vendor-reported example: Pfizer used digital workers to process European case safety reports during the COVID-19 vaccine rollout (Blue Prism)	Vendor-reported automation of European case safety reports during the COVID-19 vaccine rollout (Blue Prism). Reduces manual data entry (oboe.com).
Medical Coding & Data Extraction	- Assigning MedDRA codes to events - Pulling patient demographics, dosages from narratives	NLP, ML classifiers	Human review for complex cases Version control of code sets	Improves speed; Deloitte notes ML can extract/classify info from narrative AERs (www.deloitte.com).
Duplicate Detection	- Identifying duplicate/vaccine cohort reports	ML clustering, text-similarity algorithms	Need clear rules for 'duplicate' Monitor false positives	Enhances database cleanliness; essential with huge VigiBase growth (edit.uppsalareports.org).

PV Process	Example Tasks	AI/Techniques	CIOMS Considerations	Benefits/Evidence
Signal Detection/Signal Prioritization	- Flagging unusual drug-event combinations - Triage signals for review	Statistics (e.g. disproportionality), ML anomaly detection	High risk: patient safety impact Full validation and crosscheck needed	Potential for early signal generation (real-time surveillance) (www.deloitte.com).
Literature Monitoring	- Scanning published journals for new ADR reports	NLP, ML-based document classification	Ensure medical accuracy Manage copyright/data access	Catches reports not in safety database; reduces manual mining.
Social Media & RWD Mining	- Mining Twitter/forums for ADR mentions - EHR data modeling	NLP, deep learning	Privacy (public vs private data) Assessment of data reliability	Supplements formal reports; FDA research on ML in social media (e.g., NLP on patient posts).
Narrative Summarization (LLM)	- Generating summaries of cases or literature	Large Language Models (LLMs), GPT-like	**High precaution**: risk of inaccurate 'hallucinations' (www.scribd.com) Strong oversight needed	Can speed report writing; but CIOMS warns cautious use.
Triage/Reviewer Decision Support	- Prioritizing cases by severity - Recommending follow-ups	ML ranking models	Define use-case scope Explainability for decisions	Improves timeliness by focusing expert review on high-risk cases.
Quality Control / Audit	- Checking data completeness/consistency in database	Rule-based checks, anomaly detection	Human audit remains gold standard Supplement, not replace existing QA	Reduces simple errors; e.g., ML models can flag missing fields.

Table 1 Legend: CIOMS recommends aligning each AI application's design and oversight with its intended purpose and risk. For example, for *Case Intake Automation*, PV organisations should verify that OCR/AI systems comply with patient privacy laws (GDPR, HIPAA) and maintain audit trails. For *Signal Detection*, determine the extent and nature of expert review through the documented use-case risk assessment (CIOMS report, Chapter 4).

Data Management and Quality

AI models are only as good as the data they are trained on. **CIOMS emphasizes that AI development in PV must start with data stewardship**: assembling, curating, and securing suitable datasets. This includes internal safety databases (historical ICSRs), external sources (literature, health records), and possibly synthetic augmentation data for rare events (www.qualio.com).

Data Standardization and Integration. PV data often come from multiple international sources using different formats (e.g. CIOMS/ICH forms, local adverse event forms, literature abstracts). Before training an AI model, data should be **standardized** (e.g. using the Medical Dictionary for Regulatory Activities (MedDRA) to share coded medical information) to ensure consistency. Modern techniques like *knowledge graphs* and ontologies can help integrate heterogeneous data. For example, CIOMS notes the use of ontologies to relate drugs and events, which can improve ML features (www.scribd.com). Any data pipeline should be auditable (full logging of transformations) to meet CIOMS's governance requirements (www.qualio.com).

Data Quality and Quantity. AI thrives on large volumes, but in PV many events (especially serious ADRs) are *rare*. CIOMS advises enriching training/evaluation sets to include enough positive examples of rare signals (www.qualio.com). This could mean oversampling known ADR cases or using data from regulatory reviews. However, enrichment must be done carefully to avoid bias. All patient data used for training should be de-identified to comply with privacy regulations. Data augmentation techniques (e.g. SMOTE for tabular data or augmentation of text) can be considered to balance classes.

Example: Schmider et al. trained models using historical case source documents and corresponding safety-database answer keys, without additional annotation of the source documents (Schmider et al.). For implementation, use a separate validation dataset and define whether prospective testing is needed.

Data Privacy and Use. When AI uses external medical data (EHRs, social media, etc.), patient privacy is paramount. CIOMS recommends implementing **privacy-by-design** for AI: e.g., use of secure enclaves, encrypted data storage, controlled access, and clear consent/notice to data subjects (www.qualio.com). Patient-level data should be anonymized before ML training whenever possible. For cross-border data transfer, CIOMS notes that different countries' laws (e.g. the EU's GDPR, US HIPAA, China's Personal Information Protection Law (PIPL)) may apply concurrently, so PV systems must remain adaptable to changing regulations (www.qualio.com). The report even flags that generative AI trained on health data may inadvertently leak sensitive information, urging caution (www.scribd.com) (www.qualio.com).

Model Development and Validation

Once data are prepared, the next step is selecting and building AI models. CIOMS does not endorse specific algorithms but expects rigorous development practices.

Algorithm Selection. The choice of AI approach should match the task. Simple rule-based or linear models may suffice for structured data tasks (ICSR triage), whereas deep learning (e.g. LSTM networks) can handle unstructured narratives. Large Language Models (LLMs) like GPT-4 may offer capabilities in text summarization and interpretation, but CIOMS explicitly warns of their drawbacks: "*Particular caution should be exercised with the integration of GenAI models within PV processes.*" The "non-deterministic" nature of LLMs, opacity of training data, and risk of generating *hallucinated* outputs (false but plausible information) mean that any LLM usage requires extremely thorough oversight (www.scribd.com). In practice, early PV uses of LLMs might be limited to drafting or summarizing tasks, with final human editing.

Training and Performance Metrics. For each model, the CIOMS report emphasizes specifying in advance **how performance will be measured** (www.qualio.com). Common metrics include classification precision/recall or F1 score (for case detection), accuracy for coding, or hit-rate for signal detection. Crucially,

metrics should be tailored to PV priorities: for example, prioritizing *sensitivity* (catching true ADRs) over *specificity* may be warranted for patient safety, at the cost of more false alerts. Models should also be evaluated on *subgroup fairness*: e.g. check that the model works equally well for different age groups, sexes, or geographic populations as CIOMS notes (www.qualio.com).

CIOMS suggests *representative validation*: test data should include multiple sources (spontaneous reports, clinical study reports, literature cases) and rare event cases (www.qualio.com). If a model will operate across many products and databases, the validation set must reflect that diversity. For instance, an AE extraction model should be tested on narrative texts from different countries and languages if applicable. For rare ADRs, deliberate oversampling in the test set ensures the model's performance on these critical cases can be measured (www.qualio.com). Finally, CIOMS stresses the importance of documenting the ultimate limitations of the model: no model is perfect, so specifying conditions where it may underperform (e.g. "insufficient training data" or "extreme out-of-scope inputs") is required (www.qualio.com).

Reproducibility and Documentation. The framework calls for full **documentation** of model development: detailing the data sources used, preprocessing steps, feature engineering, model version, training parameters, etc. This is crucial for traceability and future audits. CIOMS encourages version-control of models and datasets (www.qualio.com). In practice, this means using MLops best practices: storing code in repositories, keeping records of training runs and random seeds, and linking model versions to specific deployments.

Example: In one industry survey, major firms noted that besides model performance, key challenges were obtaining high-quality training data and the need for clearer regulatory guidance on AI (pmc.ncbi.nlm.nih.gov). Addressing this, many companies now maintain PV data warehouses and data lakes with standardized formats to facilitate reproducible ML experiments.

Human Oversight and Workforce

A central thrust of CIOMS XIV is that AI should **augment** – not replace – human experts. AI tools are meant to support PV professionals, who retain ultimate responsibility.

Human Roles and Training. CIOMS distinguishes two architectures: **"human-in-the-loop"** (humans make final decisions with AI suggestions) vs **"human-on-the-loop"** (AI handles routine tasks under human monitoring) (www.qualio.com). In the former, humans review every AI output before action (e.g. a PV reviewer checks every AI-suggested ICSR entry). In the latter, AI might autonomously process many cases but humans audit its work periodically. PV organizations should decide appropriate oversight mode per application. CIOMS recommends choosing the extent and nature of human oversight through a risk-based approach, rather than assigning one mandatory review mode to all high-stakes functions (CIOMS report, Chapter 4). Document the oversight mode, quality controls, escalation rules and accountable roles for each use case.

As AI handles more tasks, PV roles will evolve. CIOMS advises planning for upskilling: safety experts may need training in AI literacy and data science concepts (www.qualio.com). Conversely, data scientists working on AI should be trained in PV regulations. Clear communication protocols must be set: e.g. if an automated case observation is flagged, how does it enter the medical review workflow? Embedding AI output fields and confidence scores in existing PV systems can help human validators focus on ambiguous cases.

Quality Control. Even with AI, traditional PV quality checks remain critical. For example, when AI performs case coding or signal prioritization, periodic *statistical review* (spot checks, double-entry sampling, etc.) should continue. CIOMS expects organizations to track AI performance in production and have contingency plans. If an AI model begins to drift (e.g. due to new data patterns), the organization must detect and address it. Many industries implement performance monitoring dashboards; PV should likewise monitor false-positive/negative rates over time.

Case Study – Automation Impact: A 2022 TransCelerate-sponsored industry survey found that PV organizations were rapidly piloting AI: *"PV organizations are very interested in and moving rapidly with planning, piloting, and production implementation of intelligent automation solutions"* (pmc.ncbi.nlm.nih.gov). The report identified challenges with suitable training data and harmonized regulatory guidance (Kassekert et al.). For workforce planning, assess training and oversight needs for each use case rather than assuming a particular headcount outcome.

Validation, Testing, and Continuous Monitoring

A robust AI deployment includes thorough validation **before** use and ongoing evaluation **after** deployment. CIOMS XIV provides guidance for both.

Pre-Deployment Validation. As mentioned, pre-deployment testing must cover a variety of scenarios. CIOMS specifically highlights the need for critical PV-specific evaluations: for example, the accuracy of identifying rare safety signals or clustering duplicates. In practice, teams should generate confusion matrices, ROC curves, and stress tests. Where possible, retrospective studies can be used: e.g., "train the model on data up to 2022 and test whether it would have caught ADRs that were confirmed in 2023." Regulatory-grade validation also requires documenting test procedures and Acceptance Criteria for moving to production.

For implementation, consider **prospective piloting** after retrospective validation. Schmider et al.'s feasibility pilot used training and test cycles; the best vendor achieved 81% case-validity accuracy against Pfizer's internal AI benchmark of 79% (Schmider et al.). This comparison does not establish human-equivalent performance or a real-time human-comparison deployment.

Performance Metrics Tailored to PV. Standard AI metrics should be defined in context: e.g., for duplicate detection, one might use precision and recall on known duplicate sets; for case coding, match-rates to expert codes. CIOMS reminds us that PV goals (catching rare but serious events) may require adjusting metrics. In high-stake applications, it may be acceptable to tolerate more false positives (lower precision) if false negatives (missed true ADRs) are minimized. All such requirements must be documented.

Continuous Monitoring and Revalidation. Perhaps most importantly, CIOMS insists on **ongoing oversight** of AI tools, not "set-and-forget." Even if a model is initially accurate, changes in reporting patterns (new drug launches, pandemic, changes in healthcare seeking behavior) can degrade performance. Therefore, teams should continuously monitor key indicators: e.g. AI vs human outcome in sampled cases, unexpected shifts in model outputs, or feedback from regulators. Any detection of drift should trigger re-training or decommissioning. Version control of models (e.g. semantic model ID including date and training data) enables comparisons over time (www.qualio.com). These practices mirror "GMP" style monitoring (sometimes referred to as "Good Machine Learning Practices") aligned with CIOMS's governance principles.

Transparency and Explainability

Transparency is a core CIOMS principle (www.qualio.com). In practice, this means that whenever an AI system is used, the organization should document its purpose and scope in accessible terms. Internal documentation (SOPs) should describe each AI model: what data it uses, what decisions it makes, and its limitations. External transparency is also important: PV staff, other business units, and regulators should know *which* analytics are AI-driven. For example, study reports or regulatory filings might note that an AI tool was used to screen cases.

Explainability Methods. While deep learning models are often opaque, modern techniques (LIME, SHAP, attention maps) can provide human-interpretable *explanations* of outputs. CIOMS suggests using these to support trust, but cautions that such methods provide *plausible* reasons, not an exact "cause." For instance, an LLM summarizing a case may highlight certain keywords as rationale. This information should be presented alongside any AI output to help reviewers understand why the model made a particular classification (www.qualio.com). Ultimately, however, human experts must recognize that explanation tools have limitations.

Stakeholder Communication. For patient advocacy and ethics reasons, organizations should also consider informing reporters or the public when AI is used in safety evaluation. For example, if patient-generated data from social media is automatically scanned, informing users of those platforms about the AI use (via privacy notices or transparency reports) may be prudent. Regulators may also want documentation on AI systems; compliance with CIOMS's transparency means that internal audit trails and reports should be ready for inspection by agencies.

Ethical and Fairness Considerations

Bias and Equity

As CIOMS highlights, AI models can **inherit biases** in data. For PV, this is particularly concerning when certain populations are underrepresented. For instance, if a safety database predominantly contains reports from one region or demographic, an AI classifier trained on it might under-detect ADRs for other groups. CIOMS recommends that training datasets **reflect the real-world populations** who will use the medicine (www.qualio.com). This may involve supplementing data from different regions or ensuring children/elderly patients appear in training sets if those groups are relevant.

During testing, the model's performance should be checked across these subgroups. For example, if an ML model is used to identify serious ADR mentions, the developer should calculate its recall separately for males vs females, or for each major ethnic group in the data. Significant disparities would need mitigation (e.g. re-weighting the training loss, gathering more data, or flagging issues in documentation). CIOMS notes that many fairness issues in PV stem from **data gaps** (e.g. fewer reports from low-income countries) (www.qualio.com). To address this, organizations could explore transfer learning or federated learning approaches to bring in smaller datasets ethically.

Ethical Usage of AI

Beyond bias, broader ethics comes into play. The CIOMS report discusses ethical considerations in relation to AI and data privacy (CIOMS report). For PV, this translates to ensuring AI use does not harm patients (through missed signals) or violate patient rights. We summarize key ethical points:

- **Informed Data Use:** Patients who report ADRs have a right to privacy; consent processes (like informed consent in a trial) should ideally include information on AI analysis components. At minimum, data protection officers should review AI projects for ethical compliance (CIOMS mentions the need for data protection impact assessments) (www.qualio.com).
- **Responsibility:** As a conservative organisational policy, teams may require human review before accepting an AI recommendation that a report is invalid. CIOMS recommends risk-based oversight; define review, quality checks, escalation and accountability for the intended use case (CIOMS report, Chapter 4).
- **Transparency to Patients:** Where possible, patients and doctors should know if their data is being processed by AI. For example, drug information leaflets or pharmacovigilance communications could note if AI is used in case follow-up (though this is not yet standard practice, it may become expected).
- **Avoiding Undue Surveillance:** Expanding AI into areas like social media monitoring must be weighed against individuals' privacy. CIOMS warns that generative AI can lead to unintended data leaks (www.qualio.com) (www.scribd.com); organizations should not feed identified patient data into external LLMs without safeguards (for example, using on-premises models only).
- **Justice:** AI deployment should not widen inequities. For example, automated PV systems should not systematically under-serve diseases prevalent in resource-poor regions due to lack of data infrastructure. Ethical frameworks encourage global PV capacity-building alongside AI adoption.

CIOMS Guiding Principles vs Implementation Steps (Table 2)

To operationalize the CIOMS framework, PV teams can follow a checklist aligning each principle with practical actions. **Table 2** below maps the seven CIOMS principles to implementation strategies, with key considerations and example references. In each case, the CIOMS report is the authoritative source for the principle, but data and tactics come from the broader literature.

CIOMS Principle	Implementation Strategies	Key References
Risk-Based Approach	• Catalog each AI use-case by impact (Classification: High/Medium/Low risk). • For high-risk systems (e.g. case triage, signal alerts), require extensive validation, documentation, and signoff by medical safety authority. • For low-risk tasks (e.g. formatting data), allow lighter controls. • Update risk classification if AI scope changes (new indications, expanded data).	(www.qualio.com) (cioms.ch)
Human Oversight	• Define human roles: decide which tasks are "human-in-loop" (e.g. final case decision) vs "human-on-loop" (AI suggests patient cases). • Determine the extent and nature of human review of *AI-flagged safety signals* through the documented use-case risk assessment (CIOMS report, Chapter 4). • Provide continuous training for PV staff on AI use. • Track accountability (who signed off on AI model use, who reviews outputs).	(www.qualio.com) (pmc.ncbi.nlm.nih.gov)

CIOMS Principle	Implementation Strategies	Key References
Validity & Robustness	• Use diverse validation sets (spont reports, trials, literature) as suggested by CIOMS (www.qualio.com). • Predefine performance criteria (sensitivity, specificity) aligned with patient safety. • Stress-test models (e.g. simulate worst-cases, missing data, data shift). • Document known limitations (e.g. “model not validated on pediatric cases”).	(www.qualio.com) (pmc.ncbi.nlm.nih.gov)
Transparency	• Maintain clear documentation of each model’s purpose, data sources, and limitations in SOPs. • Communicate AI use internally (e.g. note “AI-assisted coding” in workflow). • Use explainability tools to make model decisions interpretable (and store these explanations). • Inform regulators/auditors proactively about key AI systems.	(www.qualio.com) (www.deloitte.com)
Data Privacy	• Perform Data Protection Impact Assessments for new AI systems. • Implement “privacy by design”: de-identify patient data, secure storage (encryption), and strict access logs. • If using external/cloud AI services, ensure they comply with relevant regulations (GDPR, CCPA, etc.). • Continually monitor new privacy regulations and adapt (CIOMS warns privacy rules evolve) (www.qualio.com).	(www.qualio.com) (www.scribd.com)
Fairness & Equity	• Ensure training data covers diverse patient demographics and all relevant drug classes. • Evaluate model accuracy across sub-populations; if significant bias is found, retrain or limit use. • Address known data gaps (e.g. by merging international data) or explicitly note limitations in under-served groups. • Establish policies to avoid discrimination (e.g. AI should not reduce attention to signals from certain regions).	(www.qualio.com) (pmc.ncbi.nlm.nih.gov)
Governance & Accountability	• Assign a responsible owner (e.g. head of PV analytics) for each AI system. • Use version-control and model registries (record training data version, code, date). • Maintain audit trails of AI predictions/decisions. • Conduct periodic reviews (e.g. annual) of each AI system’s performance and controls, aligned with CIOMS advice (www.qualio.com). • Update governance procedures as AI tech or laws change.	(www.qualio.com) (pmc.ncbi.nlm.nih.gov)

Table 2 Legend: For example, under **Human Oversight**, organizations might set policy that “no signal detected by an algorithm will be reported to regulators without a safety expert’s review” (implementing CIOMS’s in-loop concept (www.qualio.com)). Under **Data Privacy**, a policy could be to avoid sending raw patient narratives to unsecured cloud AI – adhering to CIOMS’s privacy-by-design advice (www.qualio.com).

Implementation Steps and Best Practices

Building on the above principles, we outline a stepwise playbook:

1. **Define Use-Cases and Conduct Risk Assessment:** Inventory current PV processes and identify candidate tasks for AI. For each, perform a risk assessment as per Table 2. Document the intended purpose and boundaries of the AI system (akin to a "label" for the AI) (cioms.ch).

2. **Data Collection & Preparation:** Gather historical data needed (ICSR database, medical literature, etc.) and ensure quality. Create representative training and test sets with attention to rare events (www.qualio.com). Align data formats and terminology (e.g. use standardized vocabularies). Verify legal rights/agreements for data usage.
3. **Algorithm Development:** Select or train models suitable for each task. Ensure development team includes both data scientists and PV experts. For sensitive tasks (e.g. case validity), start with simpler interpretable models, advancing to complex ML only after baseline performance is achieved. Rigorously document the model and all parameters.
4. **Validation and Testing:** Conduct thorough offline evaluations. For classification tasks, compute ROC curves and confusion matrices; for coding tasks, measure coding concordance rates with ground truth. Perform subgroup analysis to check fairness (www.qualio.com). If performance meets criteria, move to "shadow mode" testing where AI operates in parallel with humans on new incoming data; confirm acceptable agreement before live deployment.
5. **Deployment with Oversight:** Integrate the AI system into PV workflow transparently. For instance, link outputs into the existing database UI, highlighting AI-confidence. Ensure a human operator can easily review and, if needed, override AI suggestions. Implement safety checks (e.g., highest-risk predictions must be double-checked). Train PV users on the system's proper use and limitations.
6. **Monitoring & Continuous Improvement:** After deployment, continuously monitor key metrics (e.g. accuracy over time, number and rate of human overrides, case processing speed). Establish feedback loops: if experts correct an AI suggestion, that corrected data should be fed back into model retraining. Schedule regular performance reviews (e.g. quarterly MLops check-ins). Any change in data patterns or goals should trigger model re-evaluation. Maintain version logs so previous models can be restored if a new model fails.
7. **Governance and Documentation:** Throughout all steps, maintain detailed documentation. This includes risk assessments, data provenance records, model validation reports, audit logs of usage, and SOP updates. Assign clear approval checkpoints: e.g., quality assurance approval before pilot, safety committee signoff before deployment. Continue to update governance policies as best practices evolve. CIOMS's "governance framework" means this is an ongoing process, not a one-time effort (www.qualio.com).

Case Studies and Real-World Examples

The **UK's MHRA Yellow Card Scheme** provides an operational example. In its March 2022 FOI response, MHRA stated that the AI tool was deployed in December 2020 and reduced manual coding of reports. MHRA described the tool as capturing information from reporters' narrative text to support analysis, subject to quality assessment; it was not used to assess the data (MHRA, FOI 22/494).

Blue Prism's vendor case study describes Pfizer's enterprise automation programme. Its target was to automate 75% of transactional processes by 2021 across functions. The reported reduction of almost 35% concerned product claim source validation, while 500,000 hours returned annually concerned the enterprise programme overall. These figures should not be presented as PV case-processing results (Blue Prism).

Academically, Schmider et al. (2019) reported composite information-extraction F1 scores of 0.72 and 0.74 for the two leading vendors, compared with 0.69 for Pfizer's internal AI benchmark (Schmider et al.). They note that this feasibility confirms AI's potential as the "commercial impetus" for PV transformation (pmc.ncbi.nlm.nih.gov). This aligns with CIOMS's statement that AI adoption is driven by escalating safety report volumes and the need for scalable solutions (cioms.ch) (edit.uppsalareports.org).

Several companies also pursue social-media PV. For example, research by Liang and colleagues showed that NLP can identify ADR mentions on Twitter with good precision in English and Chinese, suggesting supplementary real-time monitoring channels. CIOMS's documented contribution is principles and guidance for AI use in PV (CIOMS). While these projects aren't yet mature, they exemplify how AI can broaden the PV landscape beyond ICSRs.

The **Qualio blog** ("How AI is reshaping PV: CIOMS takeaways"), reflects practitioner sentiment. It reports that *"many [AI] capabilities are now integrated into routine PV workflows"*, including coding, translation, duplicate detection, signal screening, and even early LLM use (www.qualio.com). This shows industry momentum; CIOMS's framework seeks to ensure such momentum proceeds responsibly.

Discussion: Implications and Future Directions

The CIOMS XIV framework and its emphasis on rigorous implementation mark a shift toward standardized, safe AI in PV. However, several broader developments will influence the years ahead:

- **Regulatory Evolution:** CIOMS is poised to influence regulators. In parallel to CIOMS, governments are working on AI-specific laws (e.g. the EU's AI Act classifies many health-related AI as "high risk," demanding extensive evaluation). While CIOMS focuses on PV use-cases, PV professionals should note these regulatory trends. For example, recent FDA guidance documents (e.g. on Good Machine Learning Practices) and initiatives by NIST highlight the expectation of solid validation and transparency (consistent with CIOMS advice). PV teams should coordinate with legal/regulatory affairs to ensure AI tools comply with upcoming laws as well as PV regulations.
- **Global Collaboration:** Pharmacovigilance is inherently global. CIOMS itself is international, and many regulatory bodies (FDA, EMA, PMDA, etc.) are expected to consider aligning with these guidelines. The future may see joint PV-AI audits or data sharing agreements for AI development. CIOMS hints at this need by discussing cross-border data flow and harmonization (www.qualio.com). For example, evolving global standards on data privacy (like the APAC Privacy Framework) will affect how multi-national PV databases are used for AI.
- **Technological Advances:** AI technology continues to evolve rapidly. CIOMS's principles are deliberately agnostic to specific tools, so they can accommodate future breakthroughs. We can expect more use of **real-world evidence** (EHR, claims data) with AI, more sophisticated predictive models (e.g. graph neural networks linking drug-event networks), and specialized GenAI trained on biomedical text. PV systems may integrate IoT/ wearable data (e.g. patient smartphones) through AI analytics for patient-focused safety. CIOMS refers to some of these emerging areas in its "future considerations" chapter (e.g. using open LLMs for causality, or AI-driven patient alerts). Organizations should anticipate that continuous learning systems will become common, where AI tools train on incoming data streams.

- **Workforce Transformation:** Over the next decade, PV roles will increasingly demand data analytics skills. Scientists and physicians in safety departments will need training in ML concepts, software literacy, and statistical validation. Conflicts may arise between traditional PV quality units and new AI teams – requiring new governance structures as CIOMS suggests. Yet, human expertise cannot be replaced; the creative judgment of a medical reviewer remains essential. The CIOMS framework repeatedly reinforces that humans maintain the final oversight (www.qualio.com) (www.scribd.com).
- **Ethical and Social Impact:** CIOMS touches on broad ethics, but the real-world impact of AI on pharmacovigilance will be scrutinized by society. Patient advocates will demand clarity on AI's role in safety. Debates on AI bias may extend to drug safety (e.g. if an AI fails to detect a rare adverse effect mostly affecting a minority group). Organizations should proactively engage with ethicists and the public to build trust.
- **Innovation Beyond PV:** Finally, AI's influence will extend beyond core PV. Patient support programs, post-market studies, and even drug development risk management will incorporate safety analytics. Techniques like reinforcement learning might one day optimize risk minimization strategies. The CIOMS vision is broad: it envisions an ecosystem where PV data and AI interoperate to anticipate safety issues before they become widespread.

Data and Evidence Synthesis

Throughout this report, we have emphasized evidence. For instance, CIOMS's own report was based on **public consultations** and expert consensus (cioms.ch), making its recommendations robust. We have cited quantitative evidence: VigiBase growth statistics (edit.uppsalareports.org), survey findings of industry interest (pmc.ncbi.nlm.nih.gov), and pilot studies of AI in case processing (pmc.ncbi.nlm.nih.gov). However, it should be noted that much of the domain is still maturing: comprehensive public data on AI performance in PV is limited, and many implementations remain proprietary.

CIOMS describes intelligence augmentation as combining artificial and human intelligence to complement and enhance human specialist performance (CIOMS).

Statistics cited in this paper (total ICSRs, budget fractions, time savings) come from reputable sources (WHO/UMC, industry studies, peer-reviewed journals). For example, Schmider et al. describe case processing as using up to two-thirds of **internal PV resources**, based on the 2016 PVNet benchmark; this is not a fraction of total PV spending (Schmider et al.). Such data highlight why CIOMS frames AI adoption as not just optional but *necessary*, provided it's done safely.

CIOMS Working Group XIV's documented mandate is to establish and promote principles and guidance for AI in PV (CIOMS). For any proposed shared training dataset, verify the platform, participants, access rights and governance arrangements before relying on it. Track model performance and safety outcomes within each implementation.

Conclusion

The CIOMS Working Group XIV report represents a landmark in pharmacovigilance: for the first time, an international consensus defines how AI **should** be integrated into drug safety. The “implementation playbook” we’ve laid out translates those consensus guidelines into concrete steps for PV teams. Key messages are clear:

- **Balance Innovation with Caution:** AI offers unprecedented tools to manage PV’s data deluge, but must be deployed under stringent controls. A risk-based, transparent approach (as CIOMS demands (www.qualio.com)) is non-negotiable.
- **Maintain Human Judgment:** Throughout, human experts remain central. AI should assist – by taking over tedious tasks and flagging insights – but humans make final safety determinations (www.qualio.com) (pmc.ncbi.nlm.nih.gov).
- **Ensure Ethical and Systematic Governance:** Every AI initiative must be governed like a critical PV process. Documentation, validation, auditing, and adaptability to new regulations are built-in expectations (www.qualio.com).
- **Invest in People and Infrastructure:** Successful AI in PV demands not only technology but also data infrastructure (clean, standardized databases) and trained personnel. The expected ROI (speed, sensitivity) can only be realized with parallel investments in workforce training and cross-functional teams.
- **Collaborate and Monitor:** This is a global effort. Sharing best practices (e.g. via CIOMS, ICH, TransCelerate) will accelerate learning. Organizations should join collaborative forums to stay aligned with regulatory expectations. Importantly, continuous monitoring of deployed AI is as critical as its initial deployment – CIOMS makes it clear that models will evolve over time.

In summary, the CIOMS XIV framework provides a **solid foundation** for safe AI in pharmacovigilance. By following these guidelines – and by learning from early adopters and pilot studies – PV professionals can harness AI’s power to enhance drug safety surveillance. The future of PV will be one of augmented intelligence: machines helping to detect and analyze adverse events, humans ensuring those machines act in the public’s best interest.

References: This report has drawn extensively on the CIOMS XIV publication and related literature (cioms.ch) (www.qualio.com). All claims are supported by cited sources, including authoritative industry analyses (www.deloitte.com) and peer-reviewed studies (pmc.ncbi.nlm.nih.gov). The CIOMS website and working group materials (the official report) are primary sources for the new framework (cioms.ch); additional references include thought leadership from Deloitte, PV journals, and WHO.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://edit.uppsalareports.org/articles/record-growth-pushes-vigibase-past-28-million-reports
2. https://oboe.com/learn/ai-in-pharmacovigilance-1xgg32a/automated-case-intake-ai-in-pharmacovigilance-0

3. https://www.fda.gov/drugs/surveillance-post-drug-approval-activities/fda-adverse-event-monitoring-system-aems
4. https://www.deloitte.com/us/en/insights/industry/life-sciences/artificial-intelligence-in-healthcare-pharmacoviligance.html
5. https://cioms.ch/artificial-intelligence-inpv
6. https://www.qualio.com/blog/ai-pharmacovigilance-cioms-report
7. https://pmc.ncbi.nlm.nih.gov/articles/PMC6590385
8. https://www.ema.europa.eu/system/files/documents/scientific-guideline/reflection-paper-use-artificial-intelligence-ai-medicinal-product-lifecycle-en.pdf
9. https://www.ema.europa.eu/en/news/ema-fda-set-common-principles-ai-medicine-development-0
10. https://pmc.ncbi.nlm.nih.gov/articles/PMC9114066
11. https://cioms.ch/working_groups/working-group-xiv-artificial-intelligence-in-pharmacovigilance
12. https://www.scribd.com/document/857220198/CIOMS-WG-XIV-Draft-report-for-Public-Consultation-1May2025
13. https://www.scribd.com/document/969713955/ai-IN-pv
14. https://www.blueprism.com/resources/case-studies/how-pfizer-has-scaled-rpa-to-deliver-breakthroughs-that-change-patients-lives
15. https://alvigilance.siralance.com/wp-content/uploads/2025/12/WEB_2105_CIOMS_Artificial-intelligence_in_pharmacovigilance_report_EN_20251204.pdf
16. https://alt.meddra.org/htmlPages/ts_ptc_r422.html
17. https://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
18. https://www.gov.uk/government/publications/freedom-of-information-responses-from-the-mhra-week-commencing-14-march-2022/freedom-of-information-request-on-the-use-of-artificial-intelligence-ai-in-our-yellow-card-system-when-it-went-live-and-the-impact-it-has-had-on-re

THE PUBLISHER

About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

Work with IntuitionLabs

Explore AI enablement, pharma and biotech software development, data engineering and BI, and Veeva services. Contact IntuitionLabs to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

Website: https://intuitionlabs.ai

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.