Review article

Artificial intelligence in GxP-regulated pharmaceutical activities: regulatory requirements, validation, data governance and risk management

Ridvanov Ch.I.[1], Ibragimova L.N.[2]*

[1] Abdi Ibrahim Global Pharm, Almaty, Republic of Kazakhstan
[2] S.D. Asfendiyarov Kazakh National Medical University, Almaty, Republic of Kazakhstan

* Corresponding author: Liliya N. Ibragimova · ibragimova.l@kaznmu.kz

Volume 1 · Issue 1 · 2026 | Received: July 2026 | Published: 29 September 2026

Abstract

Introduction. The digital transformation of the pharmaceutical industry, together with the development of Process Analytical Technology (PAT), continuous manufacturing, and the Pharma 4.0 concept, has created favorable conditions for the broader application of artificial intelligence (AI) and machine learning (ML) in pharmaceutical development, manufacturing, quality control, and other GxP-regulated processes. At the same time, the specific characteristics of AI/ML-based systems require the adaptation of conventional approaches to validation, data governance, risk management, human oversight, and lifecycle management of computerized systems.

Objective. To systematize current scientific and regulatory approaches to the use of artificial intelligence in GxP-regulated pharmaceutical activities and to identify the key requirements for validation, data governance, risk assessment, human oversight, and lifecycle management of AI systems.

Materials and Methods. An analytical review of the scientific literature and regulatory documents was conducted. Publications indexed in PubMed/MEDLINE were analyzed together with regulatory and guidance documents issued by the U.S. Food and Drug Administration (FDA), European Medicines Agency (EMA), International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH), European Commission, and International Society for Pharmaceutical Engineering (ISPE). Particular attention was given to publications and regulatory materials issued between 2020 and 2026, while earlier foundational documents related to PAT, the Pharmaceutical Quality System, Quality Risk Management, computerized systems, and continuous manufacturing were also included.

Results. The analysis demonstrated a consistent evolution of the regulatory approach to AI, from the discussion of potential applications in pharmaceutical activities toward a risk-based governance model built around a clearly defined context of use, data governance, human oversight, model performance assessment, and lifecycle management. A major milestone was the publication in January 2026 of the joint FDA-EMA Guiding Principles of Good AI Practice in Drug Development. Analysis of an FDA Warning Letter dated April 2, 2026 demonstrated the practical application of existing current Good Manufacturing Practice (CGMP) requirements to the use of AI in the preparation of regulated pharmaceutical documentation. The principal areas of AI/ML application throughout the medicinal product lifecycle were systematized, and an author-proposed three-tier risk-based classification of AI applications in the GxP environment was developed.

Conclusions. The use of artificial intelligence does not replace existing GxP requirements but expands the scope of control to include data, the model itself, its performance characteristics, changes over time, and interaction with the user. For GxP-critical AI systems, clearly defined context of use, risk-based validation, data governance, documented human oversight, performance monitoring, and change management throughout the system lifecycle are required. Integration of AI governance into the Pharmaceutical Quality System and Quality Risk Management processes is a key prerequisite for the controlled use of artificial intelligence in pharmaceutical activities.

Keywords: artificial intelligence; machine learning; GxP; pharmaceutical manufacturing; validation; data governance; data integrity; risk management; FDA; EMA.

To cite this article: Ridvanov Ch.I., Ibragimova L.N. Artificial intelligence in GxP-regulated pharmaceutical activities: regulatory requirements, validation, data governance and risk management. Pharmaceutical Sciences and Health Products. 2026;1(1):e0003.

Introduction

Over recent decades, pharmaceutical development and manufacturing have progressively moved from predominantly empirical and discrete approaches towards scientifically grounded, risk-based and digital models of medicinal-product lifecycle management. An early stage of this transformation was the introduction of Process Analytical Technology (PAT), proposed by the U.S. Food and Drug Administration (FDA) as a system for designing, analysing and controlling manufacturing processes through timely measurement of critical attributes of raw materials, intermediates and processes to assure final-product quality [1]. Subsequently, Quality by Design (QbD), quality risk management and the pharmaceutical quality system provided a methodological foundation for deeper process understanding and a shift from testing mainly the finished product to managing quality as the product is created [2, 3].

The next stage involved continuous manufacturing (CM), real-time technologies, automated production-data collection, digital twins, cloud computing and interconnected information and manufacturing systems. Adoption of the harmonized ICH Q13 guideline established scientific and regulatory approaches to the development, implementation, operation and lifecycle management of continuous drug-substance and drug-product manufacturing [4]. Digital technologies thus became part of modern pharmaceutical manufacturing strategy rather than merely auxiliary tools for automating individual operations.

These technological changes developed into Pharma 4.0, which integrates Industry 4.0 principles into the specific regulatory environment of the pharmaceutical industry. Pharma 4.0 connects automation, the industrial Internet of Things, robotics, advanced analytics, modelling and AI in a digital ecosystem that can improve process understanding and support decisions throughout the product lifecycle [5, 6]. Unlike traditional automation, Pharma 4.0 digital maturity entails moving from simple data accumulation to interpretation and conversion into knowledge suitable for predicting process performance and product quality [5-7]. Arden et al. suggest that Industry 4.0 technologies, including AI, robotics and modern computing, can substantially change traditional manufacturing approaches, increasing flexibility, efficiency and controllability [5].

Artificial intelligence (AI) and machine learning (ML) have a particular role in this transition. Their use now extends beyond molecule discovery to formulation and process development, analysis of relationships between critical process parameters and critical quality attributes, prediction of dosage-form characteristics, continuous manufacturing control, PAT, quality control and assurance, deviation detection, predictive maintenance, pharmacovigilance and real-world data processing [7-9]. The ability of ML models to identify nonlinear relationships in multidimensional process data makes them particularly promising for PAT and intelligent pharmaceutical process monitoring and control [6, 8].

The transition from conventional software to AI/ML nevertheless creates a fundamentally new challenge for GxP-regulated environments. Computerized-system requirements have historically depended on defining intended use, documenting requirements, demonstrating compliance with specifications, controlling configuration and changes, ensuring data integrity and maintaining a validated state throughout the lifecycle [10]. Changes to GMP-critical computerized systems must be controlled, and periodic evaluation must confirm continued validation [10]. Modern pharmaceutical risk management similarly applies risk-based controls to digital technologies, computerized systems and advanced analytics [3].

Not all AI systems are self-modifying or nondeterministic, but several characteristics of modern ML models complicate conventional software validation. Outputs depend on training-data composition and quality, feature selection, model architecture, training parameters, context of use and subsequent changes, as well as code. Retraining may change decision patterns without a conventional change to explicit software rules. Generative AI adds stochastic response generation, prompt sensitivity and the possibility of factually incorrect yet plausible content. GxP therefore requires evidence not only of technical functionality but also of data suitability, model performance in a specific context of use, stability over time, change traceability and adequate human oversight [11, 12].

This issue is particularly important when model outputs inform decisions that can directly or indirectly affect medicine quality, patient safety or the reliability of regulatory evidence. Examples include predicting critical quality attributes, interpreting analytical data, identifying OOS/OOT trends, optimizing process parameters and generating pharmaceutical quality-system documents. Mathematical accuracy alone is insufficient: assessment must address the consequences of errors, input-data quality and representativeness, bias, interpretability, human review, model versioning, monitoring for performance deterioration (model drift) and lifecycle change procedures. This is consistent with ICH Q9(R1), which links the formality and depth of risk management to the significance of quality risk [3].

Regulators are moving from broad discussion of AI's potential towards specific requirements and principles for responsible use. In September 2024, the European Medicines Agency (EMA) adopted its Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, covering stages from development to post-authorization use. EMA highlights model opacity, data quality, possible bias, technical failures and the need for a human-centred approach [13].

In January 2025, FDA published draft guidance, Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products, proposing a risk-based framework for model credibility assessment in a specific context of use. Context of use (COU) is central: the same model cannot be considered abstractly “validated” regardless of its task and influence on regulatory decisions [11]. FDA states that the framework should establish and assess sufficient credibility specifically for the stated use context.

A new stage of regulatory convergence emerged in January 2026, when FDA and EMA jointly issued Guiding Principles of Good AI Practice in Drug Development. The ten principles cover AI-based evidence generation and analysis throughout the medicinal-product lifecycle, including nonclinical and clinical stages, manufacturing, post-marketing surveillance and pharmacovigilance. They emphasize human-centred design, a risk-based approach, a clear context of use, multidisciplinary expertise, data governance and documentation, appropriate model development, risk-based performance assessment and full lifecycle management [14]. Discussion is thus shifting from whether AI is permissible to how controllability, credibility and acceptable risk can be demonstrated in a specific GxP context.

Professional guidance also reflects this change in computerized-system approaches. The second edition of GAMP 5 included AI/ML provisions, and in 2025 the International Society for Pharmaceutical Engineering (ISPE) published the dedicated GAMP Guide: Artificial Intelligence. It addresses development, operation and maintenance of AI-enabled computerized systems in GxP processes while preserving patient safety, product quality and data-integrity requirements [15, 16]. This indicates the emergence of an AI lifecycle methodology extending beyond conventional computerized-system validation.

Despite rapidly increasing publications on AI in drug development, manufacturing and quality control, much of the literature focuses on the technological capabilities of individual algorithms or particular applications [6-9]. Recent work addresses AI/ML governance and validation in GxP [12], but regulatory developments in 2024-2026, dedicated GAMP guidance and joint FDA-EMA principles require an updated integrated analysis. Translating high-level human-centric design, risk-based approach, context of use, data governance and lifecycle management into concrete qualification, validation, documentation, monitoring and change-management requirements remains particularly important.

This review aims to systematize current scientific and regulatory approaches to AI in GxP-regulated pharmaceutical activities by analysing the evolution from PAT and continuous manufacturing to Pharma 4.0 and AI/ML; comparing current FDA, EMA, ICH and GAMP requirements; defining key requirements for use context, data, validation, performance assessment, human oversight and lifecycle management; and identifying unresolved issues and directions for good AI practice in pharmaceutical development, manufacturing and quality assurance.

Materials and methods

An analytical review was conducted of scientific literature and regulatory documents on AI and ML in GxP-regulated pharmaceutical activities.

Sources included scientific publications indexed in PubMed/MEDLINE and official regulatory, normative and methodological documents from FDA, EMA, the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH), the European Commission and ISPE [1-4, 10, 11, 13-16, 23].

Emphasis was placed on publications and regulatory documents from 2020-2026. Earlier sources were included when foundational to current pharmaceutical development and manufacturing approaches, including PAT [1], the pharmaceutical quality system [2], quality risk management [3], computerized systems [10] and continuous manufacturing [4]. Searching and updating of scientific and regulatory sources were completed on 25 September 2026.

Literature searches used English keywords and combinations: “artificial intelligence”, “machine learning”, “pharmaceutical manufacturing”, “GxP”, “GMP”, “pharmaceutical quality”, “validation”, “data integrity”, “quality risk management”, “process analytical technology”, “continuous manufacturing”, “Pharma 4.0”, “regulatory decision-making”, “Good AI Practice”, “context of use”, “AI lifecycle management”, “human oversight” and “generative AI”.

The review included publications on AI/ML in pharmaceutical development, manufacturing, quality control and assurance, as well as studies and analyses of AI validation, data quality and governance, risk assessment, model interpretability, human oversight and AI/ML lifecycle management [6-9, 12].

Official regulatory documents formed a separate group. They were assessed by issuing organization, publication date, status, scope and relevant medicinal-product lifecycle stage. Particular attention was given to FDA and EMA documents reflecting evolving approaches to AI in drug development and regulatory decisions [11, 13, 14, 23], and to GAMP guidance on computerized and AI-enabled systems in GxP environments [15, 16].

Regulatory and scientific sources were compared across context of use, risk-based approaches, human-centred design and human oversight, data quality and provenance,

data governance, model development and validation, performance assessment, documentation and traceability, change management, performance monitoring and AI lifecycle management [3, 11-16].

Findings underwent qualitative comparative analysis and were organized according to the evolution from PAT and continuous manufacturing to Pharma 4.0 and AI/ML, together with current requirements for quality assurance, risk, data and AI lifecycle management in GxP-regulated activities [1, 3-6, 12-16].

Results

Analysis identified several interconnected developments in pharmaceutical AI: a specialized regulatory framework; principles of good AI practice; expanding applications across the medicinal-product lifecycle; evolving requirements for data, validation and lifecycle management; and initial examples of existing CGMP requirements being applied to actual AI use in manufacturing.

Evolution of regulatory approaches to pharmaceutical AI

FDA, EMA and ISPE documents show a progression from discussion of AI/ML opportunities and risks to specific principles for model credibility assessment, lifecycle management and GxP use.

In 2023, FDA published two dedicated discussion papers. Artificial Intelligence in Drug Manufacturing addressed model governance, standards, cloud applications, validation and lifecycle maintenance in pharmaceutical manufacturing [17]. In May 2023, Using Artificial Intelligence & Machine Learning in the Development of Drug & Biological Products addressed AI/ML in research and development [18]. Both were discussion documents intended to collect stakeholder feedback.

In September 2024, EMA adopted its Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, extending consideration of AI/ML from discovery and nonclinical development to clinical trials, manufacturing and the post-authorization period [13]. The required level of control is linked to the risk of the specific system and the potential effect of its outputs on medicine quality, safety and efficacy.

FDA's January 2025 draft guidance, Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products, was the next step [11]. Unlike earlier discussion papers, it proposed a structured risk-based framework for model credibility in a defined COU. Assessment thus considers not only technical characteristics but also the specific role of model outputs in evidence concerning quality, safety or efficacy [11].

An important European development was the 2025 draft EU GMP Annex 22, “Artificial Intelligence”, prepared in the EudraLex Volume 4 revision alongside Chapter 4 and Annex 11 updates. It proposes specific requirements for AI/ML in active-substance and medicinal-product manufacturing, emphasizing intended use, training-data quality, training and validation, performance measures, test-data governance, change control, performance monitoring and human review. At the time of this review, Annex 22 remained a draft and was not an effective EU GMP annex [23].

The dedicated ISPE GAMP Guide: Artificial Intelligence was published in 2025, applying GAMP principles to AI-enabled computerized systems in GxP processes [16]. It addresses lifecycle management, allocation of responsibilities between regulated organizations and suppliers, risk management, operational monitoring and maintaining fitness for intended use.

In January 2026, FDA and EMA first presented joint Guiding Principles of Good AI Practice in Drug Development, with ten agreed principles for generating and analysing evidence throughout the medicinal-product lifecycle [14]. Its scope includes nonclinical and clinical stages, manufacturing and post-marketing activities.

The main stages of regulatory development are summarized in Table 1.

This sequence demonstrates an expanding regulatory context: from individual manufacturing and development issues in 2023 to the full lifecycles of both medicinal products and AI technologies in 2024-2026 [11, 13, 14, 16-18].

FDA-EMA Good AI Practice principles

The joint 2026 FDA-EMA document contains ten good AI practice principles. They address not only mathematical-model development and testing but also human oversight, data quality, organizational responsibility, standards compliance and lifecycle governance [14].

The first principle, Human-centric by design, requires AI development and use to align with ethical and human-centred values. It does not remove professionals from decision-making and treats human-AI interaction as part of the overall system [14].

The second, Risk-based approach, requires validation, risk mitigation and oversight to be proportionate to model risk and the specific use context. It is consistent with ICH Q9(R1) quality risk management principles [3, 14].

The third, Adherence to standards, requires AI technologies to comply with applicable legal, ethical, technical, scientific, cybersecurity and regulatory standards, including GxP [14].

The fourth, Clear context of use, requires a clear definition of the AI system's role and scope. COU is also central to FDA's 2025 draft guidance, where use context and associated risk determine the evidence needed to establish model credibility [11, 14].

The fifth, Multidisciplinary expertise, calls for involvement of specialists in both AI technology and the relevant subject area throughout the lifecycle [14].

The sixth, Data governance and documentation, requires data provenance, processing stages and analytical decisions to be documented so that information is traceable and verifiable. Privacy and sensitive-data protection must also be appropriately managed [14].

The seventh, Model design and development practices, links good AI development to appropriate model/system design and software engineering, fit-for-purpose data, and assessment of interpretability, explainability and predictive performance [14].

The eighth, Risk-based performance assessment, concerns the entire system, including human-AI interaction, rather than the isolated model. Data and performance measures must match the stated COU, and predictive performance must be confirmed using predefined testing and evaluation methods [14].

The ninth, Life cycle management, calls for a risk-based quality management system throughout the AI technology lifecycle, with planned monitoring and periodic reassessment, including when data distributions change (data drift) [14].

The tenth, Clear, essential information, requires accessible information for the intended audience about AI purpose, performance, limitations, input data, updates and interpretability or explainability of outputs [14].

These provisions are systematized in Table 2.

The joint document therefore treats the object of control as a set of connected elements-model, data, use context, user, software environment and lifecycle governance processes-rather than the algorithm alone [14].

AI applications across the medicinal-product lifecycle

Scientific publications show that pharmaceutical AI/ML applications span several lifecycle stages [5-9].

In pharmaceutical development, AI/ML analyse multidimensional experimental data, identify relationships among composition, process parameters and dosage-form attributes, optimize formulations, predict physicochemical and biopharmaceutical properties, and support QbD [5-9].

In manufacturing, AI is considered alongside PAT, continuous manufacturing and advanced analytics. Applications include predicting critical quality attributes (CQA) from critical process parameters (CPP), detecting process deviations, optimizing equipment parameters, predictive maintenance and real-time process monitoring [5, 6, 9].

In quality control, ML processes complex analytical data, including spectroscopy and chromatography, image recognition, sample classification and detection of anomalous results [6, 7, 9].

In nonclinical and clinical development, AI analyses large datasets, identifies patterns and biomarkers, models candidate characteristics, supports patient selection and analyses clinical data [8, 9, 13].

Potential pharmacovigilance and post-authorization applications include automated adverse-reaction report processing, safety-signal detection, and analysis of unstructured information and real-world data [7-9, 13, 14].

A separate area is generative AI and large language models (LLMs) for text and documentation. Potential tasks include drafting procedures, specifications, reports, document summaries and other text. A real manufacturing example documented by FDA in 2026 showed AI being used to prepare specifications, procedures and master production or control records [19].

The main application areas are presented in Table 3.

Requirements for validation, data and AI system lifecycle management

Comparison of the documents showed that regulatory and professional approaches converge on several main areas of AI system control [3, 10, 11, 13-17].

The first is defining intended use and context of use. FDA links AI model credibility assessment to the specific role of its output in decision-making. Model characteristics are therefore assessed for a particular task, rather than independently of the conditions of use [11].

The second area is risk-based validation. The extent of model and system verification should be proportionate to the risk associated with their use [3, 11, 14]. The joint FDA-EMA principles emphasize that validation, risk mitigation and oversight should be proportionate to the specific context of use and model risk [14]. A similar approach appears in the draft EU GMP Annex 22, Artificial Intelligence, which addresses the AI model’s intended use, training data quality, training and validation procedures, performance metrics and test data. The draft also provides for continuous AI system oversight, including change management, model performance monitoring and human review procedures where needed [23].

The third component is data governance. Data provenance, preprocessing operations, analytical decisions, fitness for

the intended task and traceability are essential for AI models [13, 14]. Data governance is considered throughout the AI system lifecycle.

The fourth area covers assessment of both model and overall system performance. FDA-EMA call for metrics appropriate to the stated context of use and testing of predictive performance with fit-for-purpose data [14]. Performance assessment concerns the complete system, including interaction between AI and its user.

The fifth area is change management and continuous monitoring. Beyond a one-time predeployment check, current approaches require monitoring performance during operation, periodic reassessment and consideration of data changes, including data drift [14, 16]. These requirements supplement conventional change control and periodic evaluation of computerized systems [10].

The sixth component is human oversight. In the documents analyzed, the human remains part of a controlled AI system. Their role depends on the context of use, model risk and the nature of the decision [11, 13, 14, 16].

Application of CGMP requirements to AI: the 2026 FDA Warning Letter

The regulatory review identified FDA Warning Letter No. 320-26-58 to Purolea Cosmetics Lab, published on April 2, 2026, with a separate section on inappropriate use of artificial intelligence in pharmaceutical manufacturing [19].

According to FDA, the manufacturer reported during inspection that AI agents had been used to prepare drug product specifications, procedures, and master production or control records [19]. FDA found that the AI-generated documents had not been adequately reviewed for accuracy and actual compliance with CGMP.

The Warning Letter states that an organization using AI to assist document preparation must verify the generated material for accuracy and CGMP compliance. FDA linked the absence of this control to a violation of 21 CFR 211.22(c) [19].

Inspectors also found that process validation had not been performed before products were released for distribution. A company representative responded that they had been unaware of the requirement because the AI agent used had not identified it [19].

FDA also set requirements should manufacturing resume: where AI is used in CGMP activities, including procedure and specification development, AI outputs or recommendations must be reviewed and approved by an authorized Quality Unit representative [19].

This document is therefore a recorded example of existing CGMP requirements being applied to practical AI use directly in pharmaceutical manufacturing.

Discussion

The findings indicate a transition from largely experimental use of individual AI/ML tools in pharmaceutical activities towards regulatory and quality governance of their use. The joint FDA-EMA principles indicate that AI has entered the GxP regulatory agenda. The analysis generally supports that trend but requires an important qualification: the Guiding Principles of Good AI Practice in Drug Development published in January 2026 should not be interpreted as an independent authorization to use AI in GxP or as a relaxation of existing requirements. They set principles for organizing AI use without lowering requirements for quality, efficacy, safety or the reliability of generated information [14].

The fundamental change is thus an expansion of what is controlled. For a conventional computerized system, attention centers on approved requirements, functional testing, configuration, access and change management. AI systems additionally require control of training and test data, model parameters and version, applicability boundaries, performance, user interaction and changes in effectiveness over time [10, 12, 14, 16]. Conventional computerized system validation therefore cannot automatically encompass every feature of AI/ML without adaptation.

AI validation as lifecycle evidence management

For a conventional deterministic computerized system, the expected output can generally be specified in advance for a given set of inputs. With ML, particularly generative models, this logic becomes much more complex. Outputs depend on code, training data, model architecture, tuning parameters and the actual operating environment. Generative AI introduces output variability, sensitivity to prompt wording, and the possibility of plausible but factually incorrect results [12].

For AI, it is therefore more appropriate to discuss maintaining a validated and controlled state throughout the lifecycle than a one-time declaration that a system has been validated. This requires a defined intended use and context of use, prespecified acceptance criteria, evaluation with independent data, change control and periodic confirmation that performance remains acceptable for the original task [11, 14, 16].

Model drift and data drift are particularly important. Even when initial model performance meets established criteria, changes in input data, manufacturing processes, equipment, raw materials or user behavior may gradually reduce output reliability. FDA-EMA therefore identify lifecycle management and periodic monitoring as separate Good AI Practice principles [14]. This distinguishes AI governance from an approach that verifies a model only

before deployment and then treats it as an unchanging software function.

Data governance and data integrity as foundations of AI reliability

The second fundamental issue is data quality. For AI systems, the conventional observation that output quality depends on input quality has direct GxP significance. Unrepresentative, incomplete, erroneous or uncontrolled modifications to data can produce systematically incorrect results even when an algorithm is technically implemented correctly.

AI requirements should therefore be considered alongside data integrity principles. WHO defines reliable GxP data through ALCOA+: attributable, legible, contemporaneous, original and accurate, together with complete, consistent, enduring and available [20]. WHO also explicitly connects data governance to the quality system and requires a risk-based approach throughout the data lifecycle [20].

For AI, this concept should extend beyond the final electronic document or analytical output to data provenance, preparation of training, validation and test datasets, data transformations and versions, model settings and change history. AI-generated GxP records also require identification of the source information, the initiating user, model version, AI output, human review and final approved document. Otherwise, the origin of a decision and full traceability become difficult to establish.

This approach is consistent with FDA's position on data integrity: all data used in CGMP activities must be reliable and accurate, and prevention and detection of integrity failures should be risk-based [22].

Human-in-the-loop: effective control rather than nominal participation

Key considerations are human-centeredness and the qualified professional's ultimate responsibility. The analysis further clarifies human-in-the-loop: the mere presence of a person in a process does not guarantee control of an AI system. If an employee automatically accepts generated output without sufficient information or expertise to verify it, human oversight becomes nominal.

In GxP, human control should at minimum involve understanding the AI system's purpose, limitations and known failure modes; access to source information needed for verification; authority to reject AI recommendations; and documentation of critical decisions. The depth of oversight should increase with the potential impact of AI output on product quality, patient safety or regulatory decisions [11, 14, 16].

This is especially relevant to generative AI and LLMs. Salami et al. demonstrated the potential of language models to analyze pharmaceutical manufacturing deviations and extract information from deviation reports, while also identifying hallucination risk alongside their strong information-processing capabilities [21]. Linguistic persuasiveness cannot therefore be taken as proof of factual reliability.

Significance of the FDA Warning Letter: applying existing CGMP requirements to AI

The FDA Warning Letter to Purolea Cosmetics Lab dated April 2, 2026 provides a particularly clear illustration of the practical importance of human oversight [19]. Its significance lies both in the separate discussion of inappropriate AI use in pharmaceutical manufacturing and in the nature of FDA's regulatory reasoning.

FDA did not invoke the January Good AI Practice Principles as a binding basis for the violation. It applied existing CGMP requirements, particularly those concerning the Quality Unit and manufacturing procedures. The company used AI to create specifications, procedures, and master production or control records without adequate human review. FDA treated this lack of review, within the Quality Unit's responsibilities, as a violation of 21 CFR 211.22(c) [19].

The process validation issue is especially revealing. According to the Warning Letter, a company representative attributed the absence of process validation to the AI agent's failure to identify the requirement. This demonstrates a fundamental boundary of responsibility: an omitted requirement or erroneous AI recommendation does not exempt a regulated organization and its qualified staff from CGMP compliance [19].

The practical lesson is not that pharmaceutical organizations are prohibited from using generative AI for documentation. FDA does not treat AI use as an exemption from CGMP and requires appropriate human review when it is used [19].

This demonstrates that the application of requirements to AI has moved from theory into inspection practice. However, advisory Good AI Practice principles should be distinguished from legally applicable CGMP requirements whose violation provided the basis for the Warning Letter.

Proposed risk-based classification of AI systems in GxP

Drawing on ICH Q9(R1), FDA's context-of-use approach, the FDA-EMA principles and GAMP recommendations, this review proposes a practical three-level classification of AI applications according to their potential influence on GxP decisions [3, 11, 14, 16].

This classification is not a regulatory categorization by FDA, EMA or ISPE; it is the analytical model proposed in

this review. It provides a practical interpretation of the general principle that the depth of AI evidence and control should be proportionate to the potential impact of an erroneous output.

The approach also avoids two opposing extremes: validating every AI use with the same formality regardless of risk, creating excessive regulatory burden; and treating AI as an ordinary office tool in critical GxP processes when its output actually becomes part of a regulated decision.

Potential benefits and emerging risks of AI

AI adoption offers faster processing of large information volumes and reduced staff workload. The literature supports AI's potential to analyze complex datasets, identify patterns, find similar manufacturing deviations and automate selected information tasks [5-9, 21].

However, claiming that AI eliminates human error is too categorical. It may reduce certain errors, such as those arising from manual processing of large datasets or missed recurring patterns, while creating new risks: model errors, bias, hallucinations, extrapolation beyond training data, model/data drift, excessive trust in AI output, limited supplier transparency and uncontrolled cloud-model changes [12, 14, 16, 21].

The potential benefit of AI in GxP therefore lies in redistribution of tasks: AI can perform computationally and informationally intensive work, while professionals retain responsibility for critical appraisal, interpretation and regulated decisions.

Unresolved issues

Despite substantial regulatory progress in 2024-2026, open questions include validation of foundation models accessed through external cloud services; acceptance criteria for open-ended generative outputs; supplier-managed updates outside the direct control of a GxP organization; documentation of prompts and AI-generated content; hallucination-rate and prompt-sensitivity assessment; reproducibility; and allocation of responsibility among model developers, software suppliers and regulated pharmaceutical organizations.

Continuously learning models present a separate challenge. Conventional GxP change control assumes an identifiable change, impact assessment, approval and subsequent verification. Continuous learning can blur boundaries between system versions. Critical applications therefore require either controlled, recorded model-update points or an architecture that maintains a stable validated version until the established change procedure is completed.

AI regulation thus extends traditional GxP principles to a new technological object. Quality risk management, data integrity, documentation, traceability, change management, Quality Unit responsibility and qualified human review remain central. AI additionally requires attention to training data quality, context of use, model characteristics, model/data drift and full lifecycle management.

The January 2026 FDA-EMA principles and the April 2026 Warning Letter applying existing CGMP requirements to actual AI use show AI becoming subject to systematic pharmaceutical quality governance. Pharmaceutical organizations should therefore integrate AI governance into quality risk management, computerized system lifecycles, data integrity and the pharmaceutical quality system before these technologies enter critical GxP decisions.

Future perspectives

Further AI development in GxP-regulated pharmaceutical activities will likely involve moving from conventional computerized system validation (CSV) towards broader AI lifecycle assurance, where fitness-for-use confirmation extends beyond initial implementation. Continuous assessment of applicability and performance, data/model drift, change management and documentation of all substantial lifecycle modifications will become particularly important [14, 16, 24].

Continuous model monitoring will be a key direction. AI systems used in manufacturing, quality control, pharmacovigilance and other critical GxP processes will need predefined performance indicators, acceptable variation limits, reassessment frequency and criteria triggering additional verification, revalidation or retraining [14, 16, 23, 24].

AI governance should also be integrated into the existing Pharmaceutical Quality System (PQS), as part of quality, risk, change, data, deviation, CAPA and computerized system management. This integration accords with ICH Q9(R1) and ICH Q10 by linking the level of AI control to potential effects on medicinal product quality and patient safety [2, 3].

Standardization of AI model documentation is another promising direction. Unified model cards, datasheets for datasets [25, 26], context-of-use descriptions and standardized lifecycle records could improve transparency concerning model purpose, training sample characteristics, limitations, performance, known risks and change history.

For GxP applications, these tools can be supplemented with audit trail, change management, documented human control and Quality Unit decision requirements. The separate draft EU GMP Annex 22, Artificial Intelligence, reflects movement from general principles of responsible AI use towards specialized GMP requirements for AI/ML in pharmaceutical manufacturing [23, 27].

The joint FDA-EMA publication indicates growing international regulatory convergence [14]. Further alignment of AI governance, model credibility, data governance and lifecycle management can be expected. The central challenge will remain translating broad principles into practical qualification, validation and ongoing control requirements for AI systems at different risk levels.

Limitations of this review

This study has several limitations. It is an analytical rather than systematic review and did not include formal quantitative publication selection under a PRISMA protocol. The focus was on scientific publications and regulatory documents directly relevant to AI/ML in pharmaceutical development, manufacturing and other GxP-regulated processes.

Another limitation is the rapid evolution of regulation and technology. Several FDA and EMA documents are guidance, draft guidance or reflection papers, and AI regulatory approaches are still developing. Rapid updates to commercial models, especially cloud-based and generative AI systems, may introduce risks and practical scenarios not yet reflected in published literature or current guidance.

The three-level risk-based AI classification proposed here is the authors' analytical model, not an official FDA, EMA, ICH or ISPE classification. Its practical applicability requires further discussion and testing in specific GxP scenarios.

Conclusion

The analysis shows that AI is moving beyond an exclusively experimental digital technology towards integration into regulated pharmaceutical practice. The evolution from PAT, continuous manufacturing and Pharma 4.0 to AI/ML is accompanied by changes in validation and computerized system management. Core GxP principles-quality, traceability, risk management, data integrity, documentation and qualified personnel accountability-retain their importance and extend to new technologies.

The joint FDA-EMA Guiding Principles of Good AI Practice in Drug Development, published in January 2026, marked an important step in regulatory convergence. Their ten principles identify key directions for appropriate AI use: human-centeredness, a risk-based approach, a clear context of use, multidisciplinary expertise, sound data governance, controlled model development, performance assessment, lifecycle management and transparency of essential information. These principles complement existing GxP requirements for AI-specific characteristics.

Moving from one-time AI model validation to full lifecycle management is particularly important. GxP-critical uses require assessment of algorithm functionality, data provenance and quality, context of use, model risk, validation/test dataset representativeness, human oversight, change management, monitoring, data/model drift and periodic performance reassessment. AI governance should therefore be integrated into the existing pharmaceutical quality system and quality risk management.

The FDA Warning Letter to Purolea Cosmetics Lab, published April 2, 2026, demonstrated the practical significance of these requirements. AI-generated specifications, procedures, and master production or control records without adequate human review were assessed under existing CGMP requirements. AI use does not transfer responsibility from the regulated organization to an algorithm or supplier: qualified staff and the Quality Unit remain ultimately responsible for reliable GxP documentation and compliance.

Despite progress, unresolved issues include validation of foundation models and generative AI, reproducibility of open-ended text outputs, hallucination management, model drift, cloud-based updates, data control and responsibility allocation between AI suppliers and pharmaceutical organizations. Further AI adoption in GxP requires adapting established quality mechanisms to new technological risks. Risk-based application appears most sustainable, with validation, monitoring and human oversight proportionate to the potential effect of AI output on medicinal product quality, patient safety and the reliability of regulated decisions.

Authors' Contribution

Ridvanov Ch.I. - development of the review concept; analysis of professional and regulatory aspects of artificial intelligence application in GxP-regulated pharmaceutical activities; interpretation of data; drafting and critical revision of the manuscript.

Ibragimova L.N. - development of the review concept and methodology; search, analysis, and systematization of scientific literature and regulatory documents; interpretation of the results; manuscript preparation; scientific editing and overall supervision.

All authors reviewed and approved the final version of the manuscript for publication.

Conflict of Interest

The authors declare no conflict of interest. This manuscript has not been previously published and is not under consideration for publication elsewhere.

Funding

The study received no external targeted funding.

Author information

Liliya N. Ibragimova -Candidate of Pharmaceutical Sciences, Associate Professor, Head of the Center for Pharmacy and Pharmacology of the Science and Technology Park, S.D. Asfendiyarov Kazakh National Medical University; Almaty, Republic of Kazakhstan; e-mail: ibragimova.l@kaznmu.kz; ORCID: https://orcid.org/0000-0002-8381-5330.

Chakho I. Ridvanov - Planning and Operational Excellence Manager, Abdi Ibrahim Global Pharm; Almaty, Republic of Kazakhstan; e-mail: chakho.ridvanov@aigp.kz; ORCID: https://orcid.org/0009-0003-3689-1757.

References

1. U.S. Food and Drug Administration. PAT - A Framework for Innovative Pharmaceutical Development, Manufacturing, and Quality Assurance: Guidance for Industry [Internet]. Silver Spring (MD): FDA; 2004 [cited 2026 Sep 25].

2. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. ICH Q10: Pharmaceutical Quality System [Internet]. Geneva: ICH; 2008 [cited 2026 Sep 25].

3. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. ICH Q9(R1): Quality Risk Management [Internet]. Geneva: ICH; 2023 [cited 2026 Sep 25].

4. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. ICH Q13: Continuous Manufacturing of Drug Substances and Drug Products [Internet]. Geneva: ICH; 2022 [cited 2026 Sep 25].

5. Arden NS, Fisher AC, Tyner K, Yu LX, Lee SL, Kopcha M. Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future. Int J Pharm. 2021;602:120554. doi:10.1016/j.ijpharm.2021.120554.

6. Nagy B, Galata DL, Farkas A, Nagy ZK. Application of artificial neural networks in the Process Analytical Technology of pharmaceutical manufacturing-a review. AAPS J. 2022;24(4):74. doi:10.1208/s12248-022-00706-0.

7. Batalha MAB, Pais DAM, Almeida RAE, Martinho ASG. A review of artificial intelligence and machine learning in product life cycle management. PDA J Pharm Sci Technol. 2024;78(5):604-612. doi:10.5731/pdajpst.2023.012922.

8. Suriyaamporn P, Pamornpathomkul B, Patrojanasophon P, Ngawhirunpat T, Rojanarata T, Opanasopit P. The artificial intelligence-powered new era in pharmaceutical research and development: A review. AAPS PharmSciTech. 2024;25(6):188. doi:10.1208/s12249-024-02901-y.

9. Huanbutta K, Burapapadh K, Kraisit P, Sriamornsak P, Ganokratanaa T, Suwanpitak K, et al. Artificial intelligence-driven pharmaceutical industry: A paradigm shift in drug discovery, formulation development, manufacturing, quality control, and post-market surveillance. Eur J Pharm Sci. 2024;203:106938. doi:10.1016/j.ejps.2024.106938.

10. European Commission. EudraLex Volume 4: EU Guidelines for Good Manufacturing Practice. Annex 11: Computerised Systems [Internet]. Brussels: European Commission; 2011 [cited 2026 Sep 25].

11. U.S. Food and Drug Administration. Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products: Draft Guidance for Industry and Other Interested Parties [Internet]. Silver Spring (MD): FDA; 2025 [cited 2026 Sep 25].

12. Patel B, Patel J. Validation, ethics, and lifecycle governance of AI and machine learning in GxP applications: A comparative regulatory analysis and integrated framework. AI Ethics. 2026;6:363. doi:10.1007/s43681-026-01218-9.

13. European Medicines Agency. Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle. EMA/CHMP/CVMP/83833/2023 [Internet]. Amsterdam: EMA; 2024 [cited 2026 Sep 25].

14. U.S. Food and Drug Administration; European Medicines Agency. Guiding Principles of Good AI Practice in Drug Development [Internet]. FDA; EMA; 2026 [cited 2026 Sep 25].

15. International Society for Pharmaceutical Engineering. GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems. 2nd ed. ISPE; 2022.

16. International Society for Pharmaceutical Engineering. ISPE GAMP Guide: Artificial Intelligence. ISPE; 2025.

17. U.S. Food and Drug Administration. Artificial Intelligence in Drug Manufacturing: Discussion Paper [Internet]. Silver Spring (MD): FDA; 2023 [cited 2026 Sep 25].

18. U.S. Food and Drug Administration. Using Artificial Intelligence & Machine Learning in the Development of Drug & Biological Products: Discussion Paper and Request for Feedback [Internet]. Silver Spring (MD): FDA; 2023 [revised 2025 Feb; cited 2026 Sep 25].

19. U.S. Food and Drug Administration. Purolea Cosmetics Lab - Warning Letter 320-26-58, MARCS-CMS 722591 [Internet]. Silver Spring (MD): FDA; 2026 Apr 2 [cited 2026 Sep 25].

20. World Health Organization. WHO Guideline on Data Integrity. WHO Technical Report Series No. 1033, Annex 4 [Internet]. Geneva: World Health Organization; 2021 [cited 2026 Sep 25].

21. Salami H, Smith-Goettler B, Yadav V. How can language models assist with pharmaceuticals manufacturing deviations and investigations? Int J Pharm. 2025;669:125100. doi:10.1016/j.ijpharm.2024.125100.

22. U.S. Food and Drug Administration. Data Integrity and Compliance With Drug CGMP: Questions and Answers. Guidance for Industry [Internet]. Silver Spring (MD): FDA; 2018 [cited 2026 Sep 25].

23. European Commission. EudraLex Volume 4: Good Manufacturing Practice Guidelines. Draft Annex 22: Artificial Intelligence [Internet]. Brussels: Directorate-General for Health and Food Safety; 2025 [cited 2026 Sep 25].

24. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1 [Internet]. Gaithersburg (MD): National Institute of Standards and Technology; 2023 [cited 2026 Sep 25]. doi:10.6028/NIST.AI.100-1.

25. Mitchell M, Wu S, Zaldivar A, Barnes P, Vasserman L, Hutchinson B, et al. Model cards for model reporting. In: Proceedings of the Conference on Fairness, Accountability, and Transparency. New York: Association for Computing Machinery; 2019. p. 220-229. doi:10.1145/3287560.3287596.

26. Gebru T, Morgenstern J, Vecchione B, Vaughan JW, Wallach H, Daumé H III, et al. Datasheets for datasets. Commun ACM. 2021;64(12):86-92. doi:10.1145/3458723.

27. European Medicines Agency. Good manufacturing practice: Multistakeholder workshop on expert contributions to artificial intelligence guidance development (Annex 22) [Internet]. Amsterdam: EMA; 2026 Jun 30-Jul 1 [cited 2026 Sep 25].

Table 1. Evolution of regulatory approaches to AI in pharmaceutical activities.

Year	Organization	Document	Scope	Main provisions
2023	FDA	Artificial Intelligence in Drug Manufacturing	Pharmaceutical manufacturing	AI in manufacturing, model lifecycle, standards, cloud applications and regulatory oversight [17]
2023	FDA	Using Artificial Intelligence & Machine Learning in the Development of Drug & Biological Products	Drug and biological product development	AI/ML opportunities and risks; human-led governance; data quality and reliability [18]
2024	EMA	Reflection paper on the use of AI in the medicinal product lifecycle	Entire medicinal product lifecycle	Risk-based approach, data, transparency, human oversight and model assessment [13]
2025	FDA	Considerations for the Use of AI to Support Regulatory Decision-Making for Drug and Biological Products	Data and information supporting regulatory decisions	Context of use; model risk; risk-based credibility assessment [11]
2025	European Commission / EMA GMDP Inspectors Working Group / PIC/S	Draft EU GMP Annex 22 - Artificial Intelligence	AI/ML in active substance and medicinal product manufacturing	Intended use, training data, validation, performance metrics, change control, model monitoring and human review [23]
2025	ISPE	GAMP Guide: Artificial Intelligence	AI-enabled computerized systems in GxP	Risk, lifecycle, supplier and operational control management [16]
2026	FDA-EMA	Guiding Principles of Good AI Practice in Drug Development	Entire medicinal product lifecycle	Ten common Good AI Practice principles [14]

Table 2. FDA-EMA Good AI Practice principles and associated control elements.

No.	Principle	Core meaning	GxP control elements
1	Human-centric by design	Human-centered AI development and use	Human oversight; allocation of responsibility
2	Risk-based approach	Control proportionate to model risk and context of use	Risk assessment; validation scope; control measures
3	Adherence to standards	Compliance with applicable requirements and standards	GxP; legislation; cybersecurity; technical standards
4	Clear context of use	Explicit definition of the model's role and application	Intended use; applicability boundaries; AI output impact
5	Multidisciplinary expertise	Use of multidisciplinary competencies	AI/ML; GxP; statistics; subject matter experts
6	Data governance and documentation	Traceable data provenance and processing	Data provenance; documentation; privacy; data protection
7	Model design and development practices	Appropriate model and system development	Fit-for-use data; robustness; generalizability; explainability
8	Risk-based performance assessment	Assessment of the entire system	Validation; testing; performance metrics; human-AI interaction
9	Life cycle management	System management after implementation	Monitoring; periodic review; change management; data drift
10	Clear, essential information	Accessible essential information about the technology	Purpose; limitations; data; updates; explainability

Table 3. Main AI/ML applications across the medicinal product lifecycle

Area	Potential AI/ML tasks	Related GxP aspects
Pharmaceutical development	Formulation optimization, DoE analysis, prediction of dosage form characteristics	QbD; knowledge management; model validation
Manufacturing	PAT, CQA prediction, CPP monitoring, deviation detection, predictive maintenance	GMP; process validation; change control
Quality control	Analysis of spectra, chromatograms and images; result classification; anomaly detection	Data integrity; analytical procedure performance
Clinical development	Data analysis, biomarkers, patient stratification	GCP; data quality; model credibility
Pharmacovigilance	Signal detection; report and unstructured data analysis	GVP; traceability; human review
GxP documentation	Drafting SOPs, specifications, records and other documents	Human verification; Quality Unit oversight; document control

Table 4. Proposed risk-based classification of AI applications in GxP

Level	Nature of use	Examples	Proposed controls
1 - Low risk	AI output is not directly used to make a GxP decision	Information retrieval, translation, drafting, summarizing noncritical information	Define permissible use; protect confidential data; user verification
2 - Moderate risk	AI produces material usable in a GxP process only after independent expert review	Draft SOP or deviation summary; classification or preliminary analysis of analytical data	Documented context of use; system qualification; testing; mandatory human review; audit trail/change control
3 - High risk	AI output directly affects product quality, patient safety or a critical GxP decision	CPP control, CQA prediction, critical QC data interpretation, batch release decisions, critical pharmacovigilance elements	Formal risk assessment; extended validation/model credibility assessment; independent testing; strict human oversight; continuous monitoring; lifecycle/change management