Cybersecurity for Data Integrity in the Pharmaceutical Industry: A Comprehensive Review of Threats, Regulatory Frameworks, and Mitigation Strategies

Jaydeep Patel [1*], Het Patel [2]
[1,2] Independent Researchers, USA

* Corresponding Author: **Jaydeep Patel**

Article Info

P-ISSN: 3051-3383
E-ISSN: 3051-3391
Impact Factor (RSIF): 8.40
Volume: 07
Issue: 01
Received: 09-01-2026
Accepted: 11-02-2026
Published: 13-03-2026
Page No: 55-62

Abstract
The pharmaceutical industry operates at the intersection of highly regulated manufacturing and rapidly evolving digital infrastructure, making it uniquely vulnerable to cybersecurity threats that can compromise data integrity. Data integrity, the assurance that records are attributable, legible, contemporaneous, original, and accurate, forms the foundation of Good Manufacturing Practice (GMP) compliance and patient safety. As pharmaceutical organizations increasingly adopt digital systems, cloud computing, Internet of Things (IoT) devices, and industrial control systems, the attack surface has expanded considerably. This review examines the cybersecurity threat landscape facing the pharmaceutical sector, with a particular focus on how cyberattacks undermine data integrity across the product lifecycle. The regulatory framework governing electronic records, including the United States Food and Drug Administration (FDA) 21 CFR Part 11, European Union (EU) Annex 11, and international guidelines from the World Health Organization (WHO) and the Pharmaceutical Inspection Co-operation Scheme (PIC/S), is analyzed in the context of cybersecurity requirements. Key cybersecurity strategies are discussed, including network segmentation aligned with ISA/IEC 62443 standards, zero trust architecture, encryption, access control, audit trail protection, and incident response planning. The review also explores the synergy between information security management systems (ISMS) and GxP compliance, advocating for an integrated governance approach. Emerging technologies such as blockchain, artificial intelligence, and digital twins are evaluated for their potential to strengthen both cybersecurity posture and data integrity assurance. This article provides a framework for pharmaceutical organizations seeking to align cybersecurity initiatives with regulatory expectations and operational excellence.

DOI: https://doi.org/10.54660/IJAIET.2026.7.1.55-62

Keywords: Cybersecurity, Data Integrity, Pharmaceutical Industry, 21 CFR Part 11, ALCOA+, GMP, Audit Trail, Zero Trust, ISA/IEC 62443, GAMP 5, Ransomware, Cloud Computing, Digital Twin, Network Segmentation

1. Introduction

The pharmaceutical industry is undergoing a profound digital transformation driven by the adoption of electronic batch records, laboratory information management systems (LIMS), enterprise resource planning (ERP) platforms, cloud-based quality management systems, and an expanding ecosystem of connected devices across research, manufacturing, and distribution operations. This shift from paper-based processes toward electronic systems has delivered substantial improvements in efficiency, traceability, and real-time decision-making. However, it has simultaneously introduced a constellation of cybersecurity risks that directly threaten data integrity, the foundational principle upon which drug safety, efficacy, and regulatory compliance depend. Data integrity in the pharmaceutical context encompasses the completeness, consistency, and accuracy of data throughout its lifecycle, from creation through processing, storage, retrieval, and eventual archival or destruction [1].

Regulatory agencies worldwide have codified expectations for data integrity through frameworks such as the ALCOA+ principles (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available), which serve as the benchmark against which pharmaceutical data management practices are evaluated [2]. When cybersecurity controls fail, every dimension of ALCOA+ is potentially compromised: unauthorized access can render data non-attributable, malware can corrupt records and destroy legibility, ransomware can render data unavailable, and sophisticated intrusions can alter records in ways that undermine originality and accuracy.

The scale of the cybersecurity challenge facing the pharmaceutical sector is significant. Healthcare and pharmaceutical industries experienced the highest number of data breaches compared to other sectors in recent years, and the average cost of a pharmaceutical data breach has reached approximately $4.61 million according to industry reports [3]. Ransomware remains a dominant threat, with the broader healthcare sector ranking among the top four most targeted industries globally for such attacks. Beyond financial losses, cyberattacks on pharmaceutical operations carry the potential to compromise patient safety through manipulation of manufacturing parameters, corruption of clinical trial data, or disruption of supply chain integrity.

The regulatory landscape demands that pharmaceutical companies address cybersecurity not as a standalone information technology (IT) concern, but as an integral component of their quality management system (QMS) and data governance strategy. The FDA's 21 CFR Part 11 regulation, established in 1997, sets the foundational requirements for electronic records and electronic signatures, mandating system validation, audit trails, access controls, and security measures [4]. The European Union's Annex 11 to the GMP guidelines provides complementary requirements for computerized systems. More recently, the International Society for Pharmaceutical Engineering (ISPE) has developed guidance through the GAMP 5 framework and its Records and Data Integrity guide, which explicitly acknowledges cybersecurity as a critical dimension of data integrity assurance.

This article presents a comprehensive review of how cybersecurity threats impact data integrity in the pharmaceutical industry. It examines the evolving threat landscape, analyzes the regulatory frameworks that govern electronic records and data protection, evaluates technical and organizational mitigation strategies, and explores emerging technologies that may reshape the cybersecurity and data integrity paradigm. The review is intended to serve researchers, quality assurance professionals, validation engineers, IT security practitioners, and regulatory affairs specialists working in pharmaceutical, biotechnology, and medical device organizations.

2. The Cybersecurity Threat Landscape in Pharmaceuticals

2.1. Overview of Cyber Threats

Pharmaceutical organizations face a diverse and evolving array of cyber threats that converge from multiple vectors. The sector is targeted by financially motivated ransomware groups, state-sponsored espionage actors seeking intellectual property, hacktivists pursuing political objectives, and opportunistic attackers exploiting known vulnerabilities. This hybrid threat environment reflects the unique value of pharmaceutical assets: proprietary drug formulations, clinical trial databases, patient health information, manufacturing process parameters, and regulatory submission data all represent high-value targets for different categories of adversaries.

Ransomware continues to dominate the threat landscape. Multiple high-profile incidents in recent years have demonstrated the devastating consequences of ransomware attacks on pharmaceutical operations. For example, a major pharmaceutical research and development company experienced an attack in which adversaries encrypted portions of its network, forced systems offline, and claimed to have exfiltrated over 170 gigabytes of sensitive data. In Germany, a pharmaceutical wholesaler suffered a similar incident that placed medicine deliveries to more than 6,000 pharmacies at risk. These incidents illustrate that ransomware in the pharmaceutical context is not merely an IT disruption; it can directly impede the availability and integrity of GxP-regulated data and interrupt the supply of essential medicines to patients.

Supply chain attacks represent another category of escalating concern. Pharmaceutical companies rely extensively on third-party vendors for clinical research, logistics, information technology services, and raw material supply. A breach suffered by any vendor in this extended network can cascade into the pharmaceutical organization, compromising shared data and interconnected systems. Industry surveys indicate that a significant majority of healthcare and pharmaceutical companies have been negatively affected by breaches within their third-party ecosystem [3]. The 2024 attack on a major pharmaceutical distributor in the United States, which exposed patient prescription and treatment data across at least 27 pharmaceutical and biotechnology companies, exemplifies the systemic nature of supply chain cybersecurity risk.

2.2. Operational Technology Vulnerabilities

A distinctive aspect of the pharmaceutical cybersecurity challenge lies in the convergence of information technology (IT) and operational technology (OT) environments. Manufacturing facilities rely on industrial control systems (ICS) including programmable logic controllers (PLCs), distributed control systems (DCS), and supervisory control and data acquisition (SCADA) networks to manage critical processes such as drug formulation, blending, filling, packaging, and environmental monitoring. These OT systems were historically designed for reliability and availability rather than cybersecurity, often operating on legacy platforms without built-in security features [5].

The progressive interconnection of OT and IT networks, a hallmark of Industry 4.0 initiatives, has significantly expanded the attack surface. Adversaries who gain access to manufacturing control systems can potentially manipulate process parameters, leading to unsafe drug compositions, safety incidents, or compliance violations that could result in product recalls or regulatory sanctions. The integrity of batch records, environmental monitoring data, and in-process testing results, all of which are GxP-regulated data, depends directly on the security of the OT infrastructure that generates and stores these records.

Cloud computing has added further complexity to the OT security landscape. While cloud platforms offer advantages in scalability and data accessibility, they introduce risks associated with misconfigurations, inadequate access

controls, and shared responsibility models that may not align with GxP requirements. Reports indicate that cloud resources have become primary targets for cyberattacks, with human error and misconfiguration accounting for a substantial proportion of cloud-related breaches [6]. The pharmaceutical industry's increasing reliance on cloud-hosted laboratory systems, quality management platforms, and data repositories necessitates a rigorous approach to cloud security that accounts for both cybersecurity and regulatory compliance requirements.

2.3. Insider Threats and Human Factors

Cybersecurity in the pharmaceutical industry cannot be addressed through technology alone, as human factors play a central role in both vulnerability and defense. Insider threats, whether malicious or inadvertent, represent a significant source of data integrity risk. Disgruntled employees may deliberately sabotage systems, exfiltrate proprietary data, or manipulate electronic records. More commonly, however, data integrity breaches arise from inadvertent actions: employees using shared passwords, failing to follow standard operating procedures (SOPs) for electronic record management, or falling victim to phishing attacks that provide adversaries with initial access credentials.

The pharmaceutical industry's connections to academic research institutions, which often conduct clinical trials in environments with historically less rigorous cybersecurity practices, create additional human-factor vulnerabilities. Effective mitigation requires not only technical controls but also a sustained investment in cybersecurity awareness training, a strong organizational quality culture, and leadership commitment to cybersecurity as a core business imperative rather than a peripheral IT function [1].

3. Regulatory Framework for Data Integrity and Cybersecurity

3.1. FDA 21 CFR Part 11: Electronic Records and Electronic Signatures

The United States FDA promulgated 21 CFR Part 11 in 1997 in response to the growing adoption of electronic systems in pharmaceutical manufacturing, clinical research, and regulatory submissions. The regulation establishes criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records and handwritten signatures. The core requirements of 21 CFR Part 11 encompass system validation, the generation of accurate and complete copies of records, record protection to enable accurate and ready retrieval, limited system access to authorized individuals, use of secure computer-generated and time-stamped audit trails, operational system checks, authority checks, device checks, and controls over open and closed systems [4].

From a cybersecurity perspective, several provisions of 21 CFR Part 11 are directly relevant. The requirement for access controls, implemented through unique user identification codes and passwords, addresses the need to prevent unauthorized access to electronic records. The audit trail requirement mandates the recording of all changes to regulated data, including the identity of the individual making the change, the date and time, and the reason for the change. These audit trails must be retained and available for review but must not be modifiable by ordinary users, a requirement that demands robust technical controls against both external and internal threats [7]. The system validation requirements ensure that computerized systems function correctly and reliably, which implicitly encompasses validation of security controls.

The FDA's 2003 Guidance for Industry on Part 11 scope and application clarified the agency's enforcement approach, emphasizing risk-based compliance and predicate rule requirements. More recently, the FDA has signaled its intent to modernize Part 11, with public consultations conducted to address the regulation's applicability to contemporary digital practices including cloud computing, mobile applications, and artificial intelligence. Industry observers anticipate that the revised regulation will more explicitly address cybersecurity requirements, potentially integrating Part 11 with broader data integrity regulations. The evolution toward Computer Software Assurance (CSA) as an alternative to traditional Computer System Validation (CSV) represents a parallel shift toward risk-based, ongoing verification of system performance, including security controls.

3.2. EU Annex 11 and International Guidelines

The European Union's Annex 11 to the GMP guidelines provides requirements for computerized systems used in pharmaceutical manufacturing that complement 21 CFR Part 11. Annex 11 addresses system validation, data integrity, audits, system accessibility, and security measures, mandating that companies operating within the EU maintain systems that are validated, capable of generating accurate and reliable results, and equipped with adequate security features to prevent unauthorized access or changes to data. The Medicines and Healthcare Products Regulatory Agency (MHRA) in the United Kingdom has published specific guidance on data integrity, emphasizing that data integrity is fundamental to ensuring that medicines meet required quality standards within a pharmaceutical quality system. Analyses of FDA warning letters have revealed that data integrity violations remain prevalent across the industry, with enforcement patterns reflecting increased regulatory focus on electronic quality systems and risk-based oversight [8].

The World Health Organization (WHO) and the Pharmaceutical Inspection Co-operation Scheme (PIC/S) have also issued guidance documents addressing data integrity expectations in GMP-regulated environments. These international frameworks converge on several common themes: the need for risk-based approaches to data governance, the importance of technical controls (including cybersecurity measures) to protect electronic records, the requirement for comprehensive audit trails, and the expectation that organizations foster a quality culture that prioritizes data integrity at all organizational levels. The convergence of these regulatory expectations creates a global baseline for cybersecurity practices in pharmaceutical data management, though implementation specifics may vary across jurisdictions.

3.3. The ALCOA+ Framework and Its Cybersecurity Implications

The ALCOA+ framework has become the internationally recognized standard for evaluating data integrity in regulated pharmaceutical environments. Originally developed as an acronym for Attributable, Legible, Contemporaneous, Original, and Accurate, the framework was later extended to include Complete, Consistent, Enduring, and Available. Each element of ALCOA+ carries specific cybersecurity implications. Attributability requires that every action on

regulated data be traceable to a specific individual, necessitating robust identity and access management (IAM) systems that prevent credential sharing, unauthorized access, and identity spoofing. Legibility demands that data remain readable throughout its lifecycle, which requires protection against malware that could corrupt file formats or storage media. Contemporaneity requires that data be recorded at the time of the activity, making system clock integrity and timestamp authentication critical security concerns [7].

Originality requires preservation of the first-captured data, which demands immutable storage mechanisms and protection against unauthorized modification. Accuracy requires that data be free from errors, necessitating controls against both accidental corruption and deliberate manipulation. Completeness requires that all data, including any data that has been repeated or reanalyzed, be retained, which has implications for backup integrity and protection against data deletion by malicious actors. Endurance requires that data remain intact and accessible for the required retention period, placing demands on storage infrastructure resilience and disaster recovery capabilities. Availability requires that data be accessible throughout its lifecycle for review and audit, making protection against denial-of-service attacks and ransomware a direct ALCOA+ concern.

4. Cybersecurity Strategies for Protecting Data Integrity

4.1. Risk-Based Approach to Audit Trail Protection

Audit trails represent one of the most critical data integrity controls in pharmaceutical operations, providing a chronological record of all activities related to the creation, modification, deletion, or review of GxP-regulated data. The protection of audit trails from cybersecurity threats is therefore a paramount concern. A risk-based approach to audit trail management considers the criticality of the data being protected, the potential impact of audit trail compromise on product quality and patient safety, and the likelihood of various threat scenarios [7].

Technical controls for audit trail protection should include: storing audit trail data in tamper-evident or immutable storage systems; implementing cryptographic hashing to detect unauthorized modifications; restricting administrative access to audit trail configurations through role-based access control with separation of duties; monitoring audit trail systems for anomalous access patterns; and ensuring that audit trail backup and recovery procedures maintain data integrity throughout the backup lifecycle. Organizations should also establish procedures for the periodic review of audit trails, which serves both as a compliance activity and as a cybersecurity monitoring mechanism for detecting potential unauthorized activities.

4.2. Network Segmentation and the ISA/IEC 62443 Framework

Network segmentation is a foundational cybersecurity strategy for pharmaceutical manufacturing environments, particularly where IT and OT networks converge. The ISA/IEC 62443 series of standards provides a comprehensive framework for securing industrial automation and control systems through a zone and conduit architecture. Under this model, assets are grouped into zones based on common security requirements, criticality, and functionality, while conduits define controlled communication pathways between zones. This approach creates logical security boundaries that can contain potential breaches and prevent lateral movement of threats across manufacturing systems.

For pharmaceutical manufacturers, implementing zone-based segmentation aligned with ISA/IEC 62443 enables the isolation of critical GxP systems, such as batch control systems, environmental monitoring systems, and laboratory instruments, from less critical enterprise IT systems. This segmentation limits the potential for a compromise in one area of the network to propagate to systems that directly impact product quality and data integrity. The FDA has endorsed the application of ISA/IEC 62443 standards in its operational technology cybersecurity guidance, recommending a tiered architecture (presentation, application, and data tiers) that enhances both security and network performance compared to flat network designs.

4.3. Zero Trust Architecture

Zero trust architecture represents a paradigm shift in cybersecurity, moving away from traditional perimeter-based security models that implicitly trust entities within the network boundary. Under the zero trust model, no user, device, or network connection is trusted by default; every access request must be continuously verified and authenticated regardless of the requester's location within the network. This approach is particularly relevant to pharmaceutical environments where the consequences of unauthorized access to GxP data or manufacturing control systems can directly impact patient safety.

The National Institute of Standards and Technology (NIST) has published guidance on planning for zero trust architecture and has updated its Cybersecurity Framework to Version 2.0, which provides a technology-neutral taxonomy of cybersecurity outcomes applicable to critical infrastructure sectors including pharmaceutical manufacturing [9]. The ISA Global Cybersecurity Alliance (ISAGCA) has issued a whitepaper demonstrating how ISA/IEC 62443 standards support zero trust implementation in OT environments. The key principles of zero trust, including least-privilege access, continuous verification, micro-segmentation, and comprehensive logging, align closely with the regulatory requirements of 21 CFR Part 11 and Annex 11 for access controls, audit trails, and system security. Implementing zero trust in pharmaceutical environments requires a phased approach that accounts for the unique constraints of validated systems, legacy OT devices, and the paramount requirement for manufacturing process availability.

4.4. Encryption and Cryptographic Controls

Encryption serves as a critical defense mechanism for protecting pharmaceutical data both at rest and in transit. Data at rest, including electronic batch records, laboratory results, stability data, and regulatory submissions stored in databases, file systems, or cloud repositories, should be encrypted using validated cryptographic algorithms to prevent unauthorized access in the event of a storage breach. Data in transit, whether flowing between manufacturing systems, between sites, or between the organization and external partners, requires encryption through protocols such as Transport Layer Security (TLS) to protect against interception and man-in-the-middle attacks.

Cryptographic controls extend beyond data encryption to include digital signatures for ensuring the authenticity and integrity of electronic records, cryptographic hashing for detecting unauthorized modifications to files and audit trails, and certificate-based authentication for securing

communications between systems. In the context of 21 CFR Part 11, cryptographic measures support the requirements for ensuring that electronic records are protected from unauthorized access, corruption, or loss [4]. Organizations must establish key management procedures that address the generation, distribution, storage, rotation, and destruction of cryptographic keys, with consideration for the long retention periods required for pharmaceutical records.

4.5. Access Control and Identity Management

Robust access control and identity management form the cornerstone of both cybersecurity and regulatory compliance in pharmaceutical environments. 21 CFR Part 11 requires that system access be limited to authorized individuals and that each user be assigned a unique identification code. These requirements translate into specific cybersecurity controls: multi-factor authentication (MFA) to prevent unauthorized access through compromised credentials, role-based access control (RBAC) to enforce least-privilege principles, automated account lockout after failed authentication attempts, mandatory session timeouts for inactive sessions, and comprehensive logging of all authentication events.

The management of privileged access accounts, particularly system administrator accounts that have the ability to modify audit trail configurations, system settings, and security controls, requires additional safeguards. Privileged access management (PAM) solutions that enforce just-in-time access, require additional approval workflows for sensitive operations, and maintain detailed session recordings can significantly reduce the risk of both insider threats and external attacks that leverage compromised administrative credentials. Integration with enterprise directory services and single sign-on (SSO) solutions can improve both security and usability, though organizations must ensure that these integrations are validated and do not introduce new vulnerabilities.

4.6. Incident Response and Disaster Recovery

A comprehensive incident response plan tailored to the pharmaceutical context is essential for minimizing the data integrity impact of cybersecurity incidents. Unlike general IT incident response, pharmaceutical incident response must account for the GxP implications of system compromises, including the potential need to quarantine affected products, assess the integrity of data generated during the period of compromise, and report security incidents to regulatory authorities. The incident response plan should define roles and responsibilities, escalation procedures, communication protocols (including notification of quality assurance, regulatory affairs, and executive leadership), and procedures for evidence preservation that support both forensic investigation and regulatory reporting.

Disaster recovery planning must ensure that GxP-regulated data can be restored to a known good state following a cybersecurity incident, with particular attention to the integrity of backup data. Regular backup testing, immutable backup storage (which prevents ransomware from encrypting backup copies), and geographically distributed backup repositories are critical components of a resilient disaster recovery strategy. Organizations should conduct tabletop exercises and simulated incident response scenarios that specifically address cybersecurity events affecting GxP systems, ensuring that cross-functional teams, including IT, quality, manufacturing, and regulatory affairs, can respond effectively under real-world conditions.

5. Integration of Information Security Management Systems and GxP Compliance

One of the most significant organizational challenges in pharmaceutical cybersecurity is the historical separation between information security management and GxP compliance functions. Cybersecurity implementation following frameworks such as NIST and ISO 27001 is typically managed by IT security professionals, while GxP compliance, including adherence to 21 CFR Part 11 and Annex 11, falls under the purview of quality assurance professionals. This separation often leads to duplicated efforts, gaps in coverage, and confusion about roles and responsibilities.

ISPE has recognized this challenge and established a special interest group on IT cybersecurity as part of its GAMP community of practice. The synergy between information security management systems (ISMS) and GxP compliance is significant: both disciplines are concerned with ensuring the confidentiality, integrity, and availability of data. While ISMS professionals operate across all layers of the technology stack, quality professionals typically focus on the application layer where GxP data is created and managed. Mapping controls between frameworks, such as aligning NIST SP 800-53 security controls with 21 CFR Part 11 requirements, enables organizations to leverage each discipline's expertise while avoiding duplication. This integrated approach means that rather than conducting separate verification activities for similar requirements expressed in different regulatory languages, controls can be formally tested by one group and the evidence referenced by the other [10].

Establishing an integrated governance structure requires several organizational actions: defining clear ownership of cybersecurity controls within the QMS; incorporating cybersecurity risk assessments into the overall quality risk management process; ensuring that computer system validation activities explicitly address security requirements; and establishing cross-functional review of cybersecurity incidents for their potential GxP impact. Process validation activities and the qualification of manufacturing equipment should also incorporate cybersecurity considerations, particularly where control systems and data acquisition systems are network-connected [10].

6. Vendor and Supply Chain Cybersecurity Management

The pharmaceutical industry's extensive reliance on external vendors for software, cloud hosting, integrated systems, clinical research, and logistics services creates significant cybersecurity risks that extend beyond the organization's direct control. Supply chain cybersecurity management requires a systematic approach to evaluating and monitoring the security posture of all vendors who handle, process, store, or transmit GxP-regulated data or who provide systems that directly impact product quality [2].

Vendor qualification should incorporate cybersecurity assessments that evaluate the vendor's security governance framework, access control mechanisms, data encryption practices, incident response capabilities, business continuity

planning, and compliance with relevant standards such as ISO 27001, SOC 2, and industry-specific requirements. For cloud service providers, the shared responsibility model must be clearly defined and documented, with explicit allocation of security responsibilities between the pharmaceutical organization and the vendor. Technical integrations between vendor systems and the pharmaceutical organization's IT infrastructure must be validated to prevent data integrity issues, and ongoing monitoring of vendor security performance should be incorporated into the periodic review process [4].

The growing frequency of supply chain attacks in the pharmaceutical sector underscores the importance of contractual cybersecurity requirements, including mandatory breach notification provisions, right-to-audit clauses, and minimum-security standards. Organizations should also develop contingency plans for scenarios in which a critical vendor experiences a cybersecurity incident, including procedures for maintaining operations, protecting data, and transitioning to alternative service providers if necessary.

7. Emerging Technologies for Cybersecurity and Data Integrity

7.1. Blockchain for Immutable Audit Trails

Blockchain technology has attracted growing attention as a potential solution for enhancing data integrity in pharmaceutical operations. The fundamental properties of blockchain, including decentralization, immutability, and cryptographic verification, make it theoretically well-suited for creating tamper-proof audit trails that can resist even sophisticated cybersecurity attacks. In a blockchain-based audit trail system, each record of data creation, modification, or deletion is cryptographically linked to the preceding record, creating a chain that cannot be retroactively altered without detection [5].

Several research initiatives have explored blockchain applications across the pharmaceutical supply chain, including end-to-end traceability of drug products from manufacturing through distribution, secure sharing of information between supply chain partners, and tamper-proof recording of quality control data. However, practical implementation faces challenges including scalability limitations, integration complexity with existing validated systems, regulatory uncertainty regarding blockchain's compliance status under 21 CFR Part 11 and Annex 11, and the computational overhead associated with blockchain consensus mechanisms. Technology shows particular promise for supply chain integrity applications where the distributed, multi-stakeholder nature of the problem aligns well with blockchain's architectural strengths.

7.2. Artificial Intelligence for Threat Detection and Data Integrity Monitoring

Artificial intelligence (AI) and machine learning (ML) offer significant capabilities for enhancing both cybersecurity defenses and data integrity monitoring in pharmaceutical environments. AI-powered security information and event management (SIEM) systems can analyze vast volumes of network traffic, system logs, and user behavior data to detect anomalous patterns that may indicate a cybersecurity intrusion or an attempt to manipulate GxP data. Machine learning algorithms can establish baseline patterns of normal system behavior and flag deviations that warrant investigation, enabling faster detection of both external attacks and insider threats.

In the context of data integrity, AI can be applied to detect anomalies in analytical instrument outputs, identify patterns consistent with data fabrication or manipulation in laboratory records, and automate the review of audit trails to flag suspicious activities. However, the application of AI in GxP-regulated environments requires careful validation to ensure that algorithms produce reliable and unbiased results, and organizations must address the interpretability challenges inherent in complex machine learning models. The ISPE GAMP Guide on Artificial Intelligence provides comprehensive guidance on the risk-based validation of AI systems in pharmaceutical contexts.

7.3. Digital Twins for Process Validation and Cybersecurity Testing

Digital twin technology, which creates virtual replicas of physical manufacturing processes, offers a novel approach to both process validation and cybersecurity testing in pharmaceutical manufacturing. A digital twin can simulate the behavior of manufacturing equipment, control systems, and data flows under various operational and threat scenarios, enabling organizations to evaluate the potential impact of cyberattacks on product quality and data integrity without risking actual production systems [11].

In the process validation context, digital twins can accelerate the identification of critical process parameters and their acceptable ranges, support continuous process verification through real-time comparison of actual versus simulated process data, and facilitate the assessment of process changes before implementation on physical equipment. From a cybersecurity perspective, digital twin environments can serve as testbeds for evaluating the effectiveness of security controls, conducting penetration testing exercises, and training incident response teams on realistic manufacturing scenarios. The integration of digital twin technology with process validation and cybersecurity programs represents an emerging area of research with significant potential for improving both regulatory compliance and security posture in pharmaceutical manufacturing [11].

8. Data Integrity Challenges in the Era of Digital Transformation

The digital transformation of the pharmaceutical industry has introduced a new generation of data integrity challenges that sit at the intersection of technology, regulation, and organizational culture. Legacy systems, which remain prevalent across the industry, often lack the security features necessary to meet contemporary cybersecurity requirements. Reports indicate that a significant proportion of healthcare providers and pharmaceutical companies continue to depend on outdated systems that were designed before modern cyber threats became prevalent. Migrating from these legacy platforms to modern, secure alternatives is a multi-year undertaking that requires careful planning to maintain validated states and regulatory compliance throughout the transition.

Data silos represent another challenge, as pharmaceutical organizations often operate multiple disconnected systems for manufacturing, quality, laboratory, and regulatory functions. These silos create gaps in data visibility and complicate the implementation of consistent cybersecurity controls across the data lifecycle. The proliferation of data sources, including IoT sensors, process analytical technology

(PAT) instruments, and automated manufacturing systems, has dramatically increased the volume of GxP data generated, creating challenges in ensuring the integrity of high-throughput data streams that may lack the traditional manual review points that historically served as integrity checkpoints [6].

The shift toward remote and hybrid work models, accelerated by the COVID-19 pandemic, has introduced additional cybersecurity considerations for data integrity. Remote access to GxP systems, whether for quality review, batch disposition, or regulatory submission activities, require secure authentication, encrypted communications, and endpoint security controls that may not have been part of the original system design. Remote and hybrid inspection models adopted by regulatory authorities have also placed greater emphasis on the accessibility and demonstrability of data integrity controls during inspections conducted partially or entirely through virtual means.

9. Best Practices and Recommendations

Drawing on the analysis presented in this review, the following best practices and recommendations are offered for pharmaceutical organizations seeking to strengthen their cybersecurity posture in support of data integrity.

First, organizations should adopt an integrated governance model that bridges cybersecurity and GxP compliance functions. This requires establishing clear ownership of cybersecurity within the quality management system, defining shared metrics and reporting structures, and ensuring that cybersecurity risk assessments inform quality risk management decisions [1]. The mapping of controls between cybersecurity frameworks (NIST, ISO 27001) and pharmaceutical regulatory requirements (21 CFR Part 11, Annex 11) provide a practical foundation for this integration.

Second, a risk-based approach should be applied to all cybersecurity and data integrity controls. Not all data and systems carry equal risk, and organizations must prioritize their cybersecurity investments based on a rigorous assessment of the potential impact of compromise on patient safety, product quality, and regulatory compliance. The ISPE GAMP 5 framework provides established methods for conducting such risk assessments in the context of computerized systems [12], and these methods should be extended to explicitly incorporate cybersecurity threat scenarios.

Third, organizations should implement defense-in-depth strategies that layer multiple security controls across the technology stack. This includes network segmentation aligned with ISA/IEC 62443, zero trust access controls, encryption of data at rest and in transit, endpoint protection on all systems including manufacturing equipment, continuous monitoring and anomaly detection, and comprehensive audit trail protection. No single control is sufficient; the layered approach ensures that the failure of any individual control does not result in a complete compromise of data integrity [5].

Fourth, supply chain cybersecurity must be managed proactively through vendor qualification, ongoing monitoring, contractual security requirements, and contingency planning. Organizations should require their critical vendors to demonstrate compliance with recognized cybersecurity standards and should conduct periodic assessments of vendor security performance.

Fifth, cybersecurity awareness and training programs should be mandatory for all personnel who interact with GxP systems, not limited to IT staff. Training should address phishing recognition, password hygiene, secure data handling practices, and the reporting of suspected security incidents. The effectiveness of training programs should be regularly assessed and the content updated to address evolving threat landscapes [2]. Best practices for incorporating data integrity across the pharmaceutical lifecycle emphasize the importance of data governance policies, secure data handling processes, and the systematic application of the ALCOA framework to guide documentation practices [13].

Sixth, organizations should invest in incident response and disaster recovery capabilities that specifically address the GxP implications of cybersecurity events. This includes developing procedures for assessing the data integrity impact of security incidents, establishing criteria for product quarantine decisions, and maintaining validated backup and recovery systems with immutable storage to protect against ransomware.

10. Future Directions

The cybersecurity and data integrity landscape in the pharmaceutical industry is poised for significant evolution in the coming years. Several trends are likely to shape this evolution. Regulatory modernization, including the anticipated revision of 21 CFR Part 11, is expected to more explicitly address contemporary cybersecurity challenges, potentially incorporating requirements related to cloud security, mobile devices, and artificial intelligence. The ongoing transition from traditional computer system validation (CSV) to computer software assurance (CSA) emphasizes risk-based, ongoing verification, which naturally creates opportunities for integrating cybersecurity monitoring into the continuous assurance model.

The maturation of emerging technologies, including blockchain, AI-driven security analytics, and digital twins, will create new opportunities for enhancing both cybersecurity and data integrity. However, these technologies will also introduce new regulatory questions regarding their validation, reliability, and compliance status in GxP-regulated environments [11]. Collaborative efforts between industry, regulatory agencies, and standards organizations, such as the ongoing work within ISPE, ISAGCA, and NIST, will be essential for developing practical guidance that enables innovation while maintaining the regulatory safeguards that protect patient safety.

The increasing sophistication of cyber threats, including AI-powered attacks, deepfake technologies, and the potential for quantum computing to compromise current cryptographic protections, will require pharmaceutical organizations to maintain adaptive cybersecurity programs that continuously evolve in response to the threat landscape. Investment in cybersecurity research, workforce development, and cross-industry information sharing will be critical for sustaining the industry's ability to protect the integrity of pharmaceutical data upon which global public health depends.

11. Conclusion

Cybersecurity and data integrity are inextricably linked in the modern pharmaceutical industry. The digital transformation that has enabled unprecedented improvements in manufacturing efficiency, quality control, and regulatory compliance has simultaneously created new vulnerabilities that adversaries are increasingly targeting. Ransomware

attacks that encrypt GxP data, supply chain breaches that compromise shared systems, and sophisticated intrusions that manipulate manufacturing parameters all represent direct threats to the ALCOA+ principles upon which pharmaceutical data integrity depends.

The regulatory framework, anchored by 21 CFR Part 11, EU Annex 11, and international guidelines, provides a foundation for data integrity assurance, but organizations must recognize that compliance with these regulations requires a comprehensive cybersecurity program that extends beyond the historical boundaries of GxP validation. The integration of information security management and GxP compliance, the adoption of defense-in-depth strategies, the implementation of zero trust principles, and the proactive management of supply chain cybersecurity risks are all essential components of a mature data integrity assurance program.

As the pharmaceutical industry continues to embrace digital technologies and as the threat landscape continues to evolve, the organizations that will most effectively protect data integrity are those that treat cybersecurity not as an IT responsibility but as a fundamental quality and patient safety imperative. The frameworks, strategies, and emerging technologies discussed in this review provide a roadmap for achieving this integration, but successful implementation ultimately depends on organizational commitment, cross-functional collaboration, and a culture that recognizes data integrity and cybersecurity as shared responsibilities across every level of the enterprise.

References

1. Charoo NA, Khan MA, Rahman Z. Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. Int J Pharm. 2023;631:122503. https://doi.org/10.1016/j.ijpharm.2022.122503
2. Ullagaddi P. Safeguarding data integrity in pharmaceutical manufacturing. J Adv Med Pharm Sci. 2024;26(8):64-75. https://doi.org/10.9734/jamps/2024/v26i8708
3. IBM Security. Cost of a data breach report 2025. Armonk, NY: IBM Corporation; 2025. Available from: https://www.ibm.com/reports/data-breach
4. U.S. Food and Drug Administration. Title 21 Code of Federal Regulations Part 11: Electronic records; electronic signatures [Internet]. Silver Spring, MD: U.S. Food and Drug Administration; 2017. Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11
5. Ullagaddi P. Digital transformation in the pharmaceutical industry: Ensuring data integrity and regulatory compliance. Int J Bus Manag. 2024;12(3). https://doi.org/10.24940/theijbm/2024/v12/i3/BM2403-013
6. Alosert H, Savery J, Rheaume J, Cheeks M, Turner R, Spencer C, *et al*. Data integrity within the biopharmaceutical sector in the era of Industry 4.0. Biotechnol J. 2022;17(6):2100609. https://doi.org/10.1002/biot.202100609
7. Patel B, Patel J. Risk-Based Approach for Audit Trail in Pharmaceutical Industry: Ensuring Data Integrity Under FDA and EU Regulations. Int J Manag IT Eng. 2025;15:18-31. https://doi.org/10.5281/zenodo.17245470
8. Ingale MH, Tayade MC, Patil YP, Salunkhe R. Data integrity violations in the pharmaceutical industry and regulatory measures. Int J Pharm Qual Assur. 2023;14(2):416-420. https://doi.org/10.25258/ijpqa.14.2.29
9. National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity (Version 2.0). Gaithersburg, MD: NIST; 2024. https://doi.org/10.6028/NIST.CSWP.29
10. Patel B, Pacha N, Patel J, Singh A. Digital twin technology and process validation in pharmaceutical manufacturing: Bridging virtual simulation and regulatory compliance for next-generation drug production. Preprints. 2026:2026021643. https://doi.org/10.20944/preprints202602.1643.v1
11. Pedro F, Veiga F, Mascarenhas-Melo F. Impact of GAMP 5, data integrity and QbD on quality assurance in the pharmaceutical industry: How obvious is it? Drug Discov Today. 2023;28(11):1-9. https://doi.org/10.1016/j.drudis.2023.103750
12. International Society for Pharmaceutical Engineering. GAMP 5: A risk-based approach to compliant GxP computerized systems. 2nd ed. Tampa, FL: ISPE; 2022. Available from: https://ispe.org/publications/guidance-documents/gamp-5
13. Gokulakrishnan D, Venkataraman S. Ensuring data integrity: Best practices and strategies in pharmaceutical industry. Intell Pharm. 2025;3(4):296-303. https://doi.org/10.1016/j.ipha.2024.09.010

How to Cite This Article

Patel J, Patel H. Cybersecurity for data integrity in the pharmaceutical industry: a comprehensive review of threats, regulatory frameworks, and mitigation strategies. International Journal of Artificial Intelligence Engineering and Transformation. 2026;7(1):55–62. doi:10.54660/IJAIET.2026.7.1.55-62

Creative Commons (CC) License

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.