VIEWPOINT

ENSURING DATA INTEGRITY IN A CLOUD – DRIVEN PHARMACEUTICAL WORLD

Infosys®
Navigate your next

Introduction

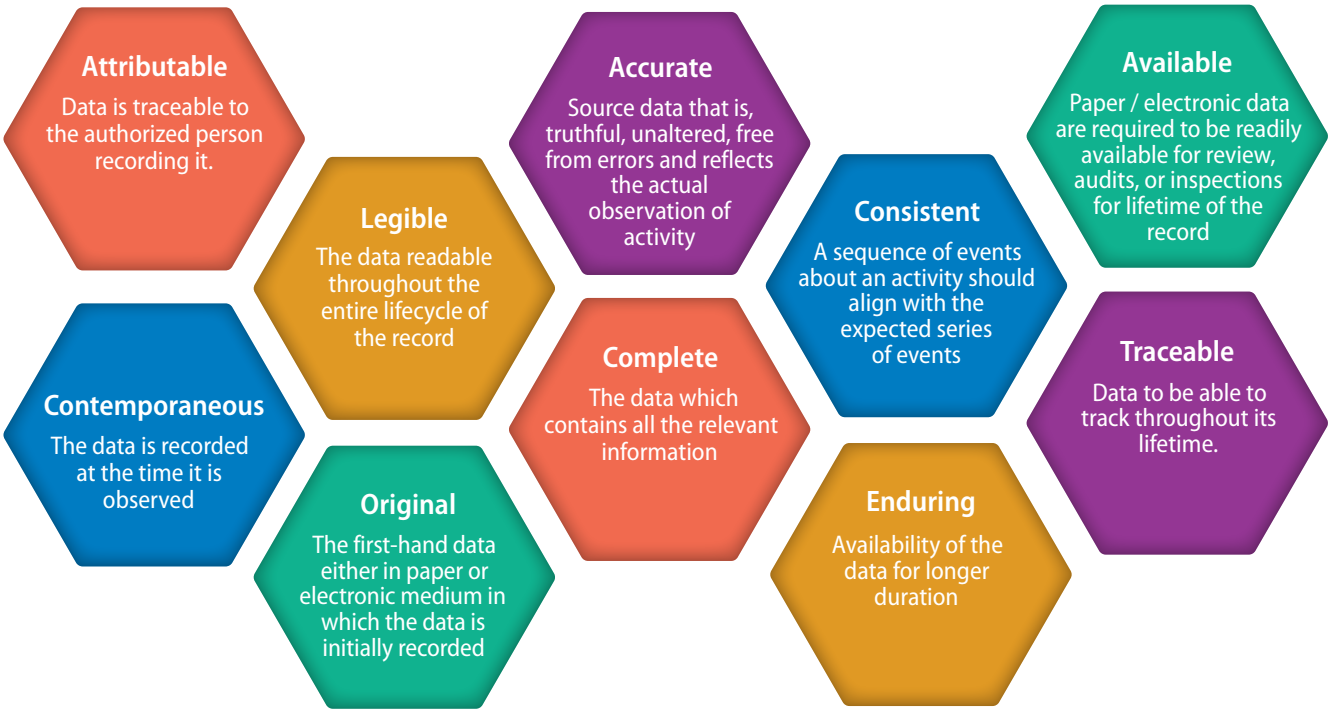
The pharmaceutical industry is at the forefront of a digital revolution, often referred to as Pharma 4.0 (The term coined by the International Society of Pharmaceutical Engineering (ISPE)).This transformation aligns with the principle of Industry 4.0 where automation, connectivity, and advance technologies are reshaping manufacturing and quality processes. At the heart of Pharma 4.0 lies Cloud computing, a technology that enables real time data sharing, scalability, and collaboration across global operations.

Cloud - based systems are important part of pharma 4.0, driving innovations in areas such as IoT - enabled manufacturing, advanced technology including AI and machine learning, and digitalized QMS (Quality Management Systems). However, the shift from traditional on-premises system to interconnected cloud environments also introduce new challenges especially maintaining Data Integrity - A pillar to ensure Regulatory Compliance, Product Quality and Patient Safety. This POV explores role of cloud computing and outlines the actionable strategies to ensure the Data Integrity in the cloud-driven era.

Importance of Data Integrity in Pharmaceuticals

Data integrity is the fundamental necessity to ensure the Regulatory Compliance, Product Quality and Patient Safety. Regulatory agencies like FDA, MHRA, EMA etc. adhere to the ALCOA++ principles. These principle states the data must be:

ALCOA ++ Principles



The shift to cloud-based systems includes third-party vendor involvement and increased system interconnectivity, which require more attention to meet the data integrity requirements.

Contrast of Data Integrity between On-Premise and Cloud Systems

Pharmaceutical companies have traditionally relied on On-premises systems to maintain full control over their IT infrastructure. However, understanding the difference between these two approaches is critical to addressing the concerns of handling Data Integrity.

Parameter	On-Premise	Cloud
Control and Accessibility	These systems provide organization with complete control over their infrastructure offering high customization. However, accessibility is often restricted to internal networks, limiting remote collaboration.	These systems enable global accessibility and seamless collaboration. However, data management will be the shared responsibility between CSPs and regulated organization.
Cost and Scalability	Require high initial investment in hardware and software. Scalability is limited and involves additional infrastructure costs.	Operates pay-as-you-go model, Scalability is virtually unlimited allowing organization to adapt quickly to evolving business needs.
Business Continuity	Relay on internal backup, which may fail during disaster	Offers robust disaster recovery option through geographically distributed data centers.
Data Integrity	ALCOA++ principles can be easily implemented however, reliance on manual process and legacy systems can increase the risk of data errors and Good Documentation Practices.	Advance tools for automation and monitoring will help to maintain ALCOA++, however challenges like unauthorized access and third-party dependence require robust governance.

Challenges to Data Integrity in Cloud Environments:

System under third-party control

Since vendor manages the data storage and the cloud system completely, few challenges faced are:

- Limited access to vendor operations
- Alignment between Vendor QMS and regulatory requirements
- System Updates and changes

Data ownership and Accountability

A shared responsibility between cloud service providers (to manage infrastructure & storage) & regulated organization (to ensure Data Integrity). Few Key Risks are:

- Loss of control over data management.
- Vendor lock-In.
- Lack of real-time monitoring and incident response.
- Intellectual property protection.

Vulnerability Issues

Since the cloud systems are more dependent on the third party for additional support required, there may be chance of cybersecurity risks. Hence its important to ensure security measures & protect the data from unauthorized access. Some of the key risks are:

- Data breaches and theft
- Improper data encryption
- Insider threats
- Ransomware and malware attacks

Regulatory Oversight

Cloud providers may lack understanding the pharmaceutical regulations which requires regulated organization to educate & enforce compliance standards through audits & agreements. Some of the key risks are :

- Validation of cloud systems.
- Data residency & its regulations.
- Process delays during regulatory Inspections/ audit

Real-Time Data Complexity

As cloud systems were enable real time data transfer between the device and systems, maintaining data accuracy and reliability at high speed becomes more challenging. Below are the key risks to be considered:

- High latency and Network dependence
- Disaster recovery and Business continuity.

Improving effectiveness of Data Integrity in Cloud systems:

1. **Selection of Right Cloud Partner:** Choose a cloud provider with demonstrated expertise in GxP compliance and are globally certified. From technical standpoint, vendor selection should be based on usage of systems that support open standards, APIs and interoperability to ensure compatibility with other platforms. From quality standpoint, conduct audits and risk assessment to evaluate their compliance in QMS (definition and adherence) and infrastructure. Also, a good practice is to include data integrity requirements and protection of intellectual property clause in the SLAs (Service Level Agreements).

2. **Implement Robust Validation Process:** Validate all the cloud-based systems with risk-based approach as per GAMP 5 and implement automated monitoring tools. Maintain robust documentation to address the changes and these should be evaluated during periodic review.

3. **Increase the Data Security:** Implement advanced data security measures like encryption, MFA (Multi-Factor Authentication) and intrusion detection systems. Regulated organization should ensure back up system and disaster recovery plans are validated and tested frequently. Use of automated tools will be more effective to detect the data integrity issues in real time and prevent vulnerability issues.

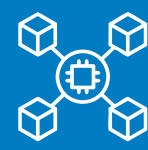
4. **Establish an effective Governance Framework:** Regulated organizations should ensure that the CSP (Cloud service provider) develop comprehensive data governance policy that defines roles & responsibilities and procedure for maintaining data integrity across the cloud systems. Most importantly, regulated organizations should ensure the cloud systems are 21 CFR Part 11 compliant.
5. **Achieving Resilient Connectivity:** High speed network connectivity is critical for the smooth functioning of the cloud-based systems. This can be achieved by implementing redundant connections, edge computing solutions, adopting content delivery networks, and by using network monitoring tools.
6. **Strengthening Vendor Collaboration:** Regulatory audits demand comprehensive and timely access to data and systems. In a cloud-based support, ensuring vendor support during the audit is crucial to maintain the compliance and avoiding delays. This can be done by establishing clear SLAs, partnered with audit-ready providers with a collaborative audit planning approach.

Use of Advanced Technologies to Enhance Data Integrity in Cloud Systems:

Adopting advanced technologies is key to maintaining and enhancing Data Integrity in a cloud-driven environment. Below are some of the advanced technologies which helps to maintain the Data Integrity.

Artificial Intelligence & Machine Learning (AI/ML)

AI/ML algorithms help to detect anomalies in real-time, reducing risk of data tampering or errors. It also helps to perform predictive analysis to identifying potential risks before they occur, enabling effective data management.



Block Chain Technology

This technology ensures data integrity by creating audit trails, ensuring transparency and tamper proof records. It is predominantly useful for ensuring traceability and compliance in pharmaceuticals supply chains

IoT Integration

IoT device enable real-time data capture, essential for monitoring critical parameters in manufacturing and supply chain. Ensuring the integrity of tools in cloud systems require robust validation and security measures.

Cloud-native Security Tools

CSPs provide advanced tool for encryption (Ex. AWS Key management service), continuousness monitoring (Ex. AWS Cloud trail), & automated compliance reporting (Ex. Prisma Cloud by Palo Alto Networks). These tools help in ensuring the data remains secure and adhere to ALCOA++ Principles.

Conclusion

As pharmaceutical industry embraces the cloud, ensuring data integrity becomes both a challenge and an opportunity. In this transformation, ensuring data integrity must remain a top priority.
Companies must implement robust strategies including data encryption, regular backups, access controls, thorough data validation, comprehensive audit trails, robust training programs for employees, and strict adherence to regulatory guidelines like 21 CFR Part 11, all while leveraging the cloud provider's security features to maintain the accuracy, completeness, and consistency of critical pharmaceutical data throughout its lifecycle By adopting a strategic approach to cloud adoption, companies can build systems that are not only complaint but also secure efficient and trustworthy.

Authors

Vinayak Shivaram Hegde,

Senior Consultant - Lifesciences Domain Consulting Group

Nitin Umapathy Kashyap,

Senior Consultant - Lifesciences Domain Consulting Group

For more information, contact askus@infosys.com

Infosys®
Navigate your next