

Equipment Data Storage Compliance for Pharmaceutical Industry

By:

Pavithran Ayyala

*Chief Information Officer & VP-Digital
(SME – Pharma Industries)*



ENHANCING DATA MANAGEMENT PRACTICES

FOSTERING AWARENESS AND BEST PRACTICES

A recent USFDA-483 inspection highlights critical concerns on Data Storage Capability, Backup, and Primary Data Management.

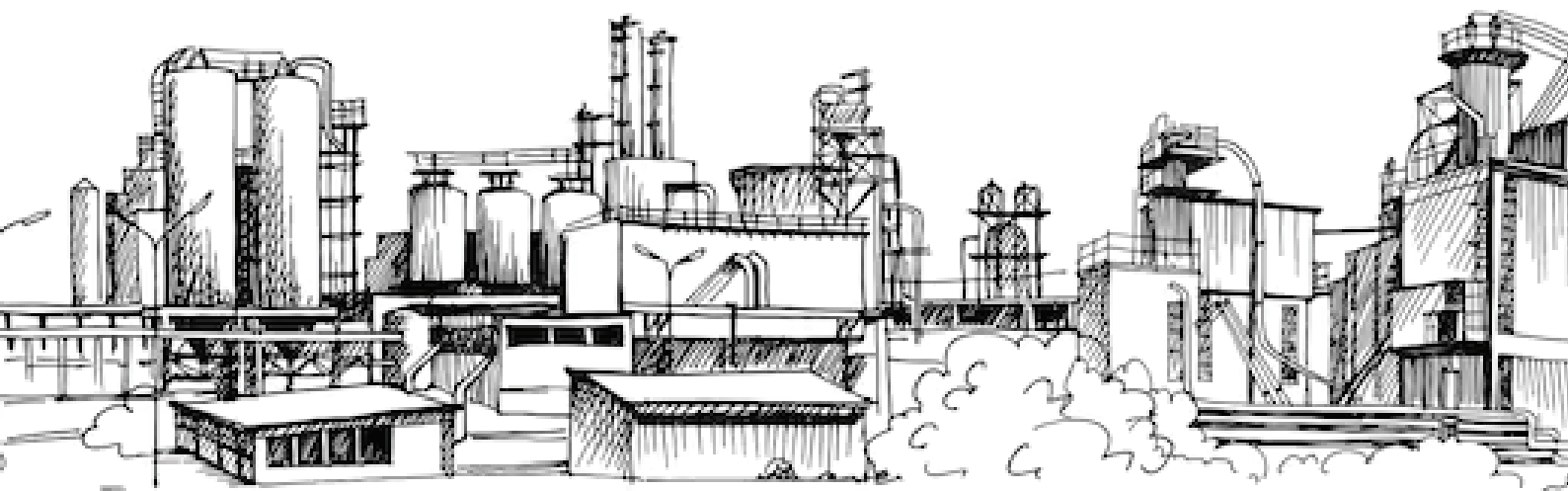


During the review of your equipment and software, it was observed that the firm was not aware of the Equipment Data Storage compliances. Consequently, your systems do not review or backup the electronic data generated and stored on the equipment using printer printouts as primary data. Per your firm's assessment, the data capability storage for this equipment is up to 1000 tests, after which the data is overwritten with the most recent data. After our identification of this discrepancy during the inspection, your firm initiated a deviation investigation....

Briefly, the USFDA emphasizes that if an organization's equipment possesses data storage capability, it is essential to have electronic data as the primary source of information. Consequently, such organizations must implement appropriate measures to ensure the security and integrity of data arising from different sources.

This observation highlights a potential compliance gap many organizations must be aware of.

As technologies continue to evolve and play an integral role in organizations' processes, it is paramount that we stay informed, adapt, and follow practices accordingly. Ignoring or overlooking data storage capabilities could seriously affect data integrity, regulatory compliance, and patient safety.





Awareness Initiatives Audience

CSV, ITQA, Compliance, and GxP

An **FDA 483** observation, or "inspectional observation," is a notice issued by the FDA to highlight potential regulatory violations identified during a routine inspection. One can relate such an incident to a company's operational facility, equipment, processes, controls, products, employee practices, records, etc.

PLAN OF ACTION

To address the concerns mentioned above and align with regulatory compliances, it is crucial for organizations to

1 ASSESS DATA STORAGE CAPABILITIES



Identify the equipment and software used for various operations with data storage capabilities. It is essential to have a comprehensive understanding of these capabilities to ensure effective and error-free data management.

2 ESTABLISH ELECTRONIC DATA AS PRIMARY



Recognize electronic data as the primary source of information for all operations and processes. More importantly, the companies should view the physical print materials as secondary storage rather than the primary source of centralized digitized data.

3 IMPLEMENT DATA SECURITY MEASURES



Devise and implement appropriate measures to secure electronic data generated and stored on the equipment. Data storage may include access controls, encryption, regular backups, and disaster recovery plans

4 FOSTER A CULTURE OF COMPLIANCE



Promote a compliance-centric culture within the organization, where all stakeholders know the importance of data integrity and the necessary measures to achieve it. Companies can foster such awareness through training programs, regular audits, and effective communication channels.

By proactively setting clear and transparent expectations, organizations can strengthen their compliance posture, minimize the risk of non-compliance, and uphold the highest quality standards in the industry.

Pharmaceutical companies must consider the following recommendations



Raise Awareness

Ensure that all personnel, including CSV, ITQA, Compliance, and GxP teams, understand the importance of electronic data storage and backup as the primary source.



Conduct Equipment Assessment

Perform a comprehensive assessment of all equipment and software used within the organization to determine their data storage capabilities.



Conduct Training Programs

Provide comprehensive training programs to educate employees about the importance of data integrity and regulatory compliance. Design and implement specific data management, storage, and backup measures. Ensure the training programs deliver measurable goals and cater to different job roles and responsibilities.



Ensure Data Security:

Develop and implement appropriate measures to secure electronic data generated and stored on equipment. Such practices may involve implementing access controls, encryption, regular backups, and disaster recovery plans to protect against data loss or unauthorized access.



Implement Data Management System

Establish a robust data management system that prioritizes electronic data as the primary source. This system should include data review, backup, retention, and retrieval protocols.



Foster Collaboration

Encourage collaboration and communication among departments involved in data management, compliance, and quality assurance.



Stay Updated on Regulations

Continuously monitor and stay updated on regulatory guidelines and expectations for data management, storage, and backup. Ensure enough room for regular internal audits to ensure everyone follows statutory compliance and global industry standards.



Learn from Industry Best Practices

Stay informed about industry best practices for data management. Be informed about the latest trends and leverage other pharmaceutical companies' insights to enhance your data management strategies.



Update Policies and Procedures

Review existing policies & procedures to reflect the expectation of considering electronic data as the primary source. Clearly define the roles and responsibilities of personnel involved in data management, backup, and security.

By implementing the abovementioned recommendations, pharmaceutical companies can strengthen their data management practices. It will also help establish the compliance ecosystem with regulatory expectations, safeguard data integrity, and contribute to the safety and efficacy of their products.

Utthunga Technologies is a leading Product Engineering and Industrial Solutions company. We develop cuttingedge digital products and solutions for industrial OEMs, Industries, ISVs, and Service Providers. Utthunga is a dominant name in software development, firmware & hardware development, IIoT applications, IT-OT integration, field device integration, industrial communications, security engineering, and testing services. Our services and solutions are highly popularized across industries like Process, Factory, Power, Building, and Mobility.

