Author: Orlando Lopez

Published on IVT Network (www.ivtnetwork.com)

GXP Volume 26, Issue 1 – January 2022

DATA INTEGRITY STRATEGY DOCUMENT ESSENTIALS

INTRODUCTION

This article will cover the essential elements of the Strategy Document. Even many of the references in this article are related to manufacturing; this article applies to all GxP regulations (1).

Worldwide regulatory agencies acceptance of data (2) from manufacturers for decision-making depends on the regulatory agencies ability to verify the reliability of the data during submissions and on-site inspections to assess products quality. One characteristic of reliable data is its integrity. From the context of data engineering, data integrity (DI) is the property that data has not been altered in an unauthorized manner (3).

Based on Reference #2, "High data integrity means data hasn't been altered in an unauthorized manner, corrupted or misused. Achieving data integrity requires asking questions such as how is the data being transferred? and what is the risk of corruption during that process? Is data access limited to the authorized people and the correct access right, or has sensitive data been compromised? Does the data remain consistent (4) during routine updates?" (5)

Data is infrequently static. After the data is collected, it is usually modified. Once DI is successfully implemented, the data must be frequently reviewed. The DI Governance is the system, with written and approved plans and procedures, with the overall control approach to ensure data integrity in the Good Manufacturing Practices (GMP) areas.

The DI Governance encompasses the system by which a regulated entity (6) operates under the principles (7) of DI and the mechanisms by which it, and all regulated users (8), are held to account for DI in all GMP related activities, including during the design, operation and monitoring of the pharmaceutical and biologics manufacturing processes and systems.

Ethics, risk management, compliance and administration are all elements of the DI Governance. It also includes defining roles and responsibilities, measuring and reporting, addressing data ownership, and the actions to resolve any DI issues identified throughout the system and data lifecycle.

A strong management commitment must direct the DI Governance to appropriate organizational culture and behaviors and understand data criticality, data risk and data lifecycle (7). The structure of a DI Governance consists of the strategy, policy, plan, procedures, and work instructions. This system should be integral to the regulated user Pharmaceutical Quality System.

STRATEGY DOCUMENT

The DI Strategy Document, as part of the DI Governance system, is a critical record providing practical DI expectations and data management to ensure integrity in the GMP data as part of the regulated entity. The general principles of good documentation practices (GDPs) can describe the DI expectations for the data lifecycle, ensuring its integrity regardless of media.

Author: Orlando Lopez

Published on IVT Network (www.ivtnetwork.com)

GXP Volume 26, Issue 1 – January 2022

Table 1 provides the expectations and critical elements of the records management processes. These essentials apply to paper and electronic records (e-records) and are the critical elements in the strategy document.

After developing the DI Strategy and Policy documents, the assessments of existing electronic systems (9) managing GMP e-records provide the landscape of the e-records management into these systems. Based on the results of the assessments, the appropriate technological and/or procedural controls are carried out, remediating existing and implemented electronic systems compliant to the e-records integrity.

On new electronic systems, an assessment of the electronic system vendor provides the approach to the e-records management by the application to be acquired. Based on the assessment results, the appropriate technological and/or procedural controls are carried out, implemented electronic systems compliant to the e-records integrity.
The strategy document provides an approach that ensures the integrity of the data is maintained for all records (10) required under the GMP. It includes what will be acceptable as data reliability to accurate and complete reporting of all data.

The assessment of the effectiveness of DI implemented is measured by reviewing a complete data set generated through processes throughout the data life cycle (11).

DATA INTEGRITY BY DESIGN

The expectations and supporting controls listed in Table 1 performed throughout the retention period of the data are the essential elements of data integrity by design (12). These apply to paper records and e-records. For example, in a typical manufacturing environment, sensor data (13) becomes a GMP e-record when the sensor data is captured and saved to satisfy a GMP requirement.

As depicted in Table 1, the integrity of GMP data should be safeguarded throughout the retention period in four stages of the data flow: during data entry or collection, data storage, data transmission, and data processing.

Stages of the Data Flow	Expectations	Supporting Controls
Data entry or collection Def. - The process of placing an object under records management control for disposition and access purposes (14).	• Systems should be designed for the capture of data accurately (15) whether acquired through manual or automated means. • Data should be recorded, documented, or saved when it is generated, with reliable evidence that this was done.	• Establish policies, plans, and procedural control to implement and enforce the data integrity procedural and technological controls. • Address records ownership throughout the records lifecycle. • Validate systems with particular attention to any system used to produce data.
Data storage Def. - Data storage is the recording (storing)	• Qualify repositories of records for their intended use. • Retain records in their original format.	

Author: Orlando Lopez

Published on IVT Network (www.ivtnetwork.com)

GXP Volume 26, Issue 1 – January 2022

STAGES OF THE DATA FLOW	EXPECTATIONS	SUPPORTING CONTROLS
information (data) in a storage medium.	• Original records (or a true copy (16)) are subject to periodic review by qualified personnel. • A true copy must undergo a qualified conversion process that maintains data integrity. • Records should be traceable to the original records by documenting changes to the original records. • Organize and record the execution and purpose of test procedures in an interpretable and traceable way. • Records should be legible, with no parts of the data obscured or removed. If archived, they must be retrievable in a timely way. • Backup must be performed for disaster recovery to data, metadata, and system configuration settings on storage. The backup copy must be a true copy of the backed-up records. • User access controls shall be configured and enforced to exclude unauthorized access to, changes to and deletion of data.	• Records must be generated and maintained under the oversight of a pharmaceutical quality system, ensuring that the data is complete and has not been altered in an unauthorized manner. When altered in an authorized manner, the alteration is traceable to the original data. • Have systems and procedures to ensure that records are reliable (17). • Security must be established at several levels: physical security and logical security at network, data server, and application.
Data transmission Def. - Data transfer is the process of transferring data between different data storage types, formats, or computer systems (18).	• Qualify the infrastructure in which records are transmitted. • Enable controls to ensure the transmitted data have remained unaltered during transmission. • Ensure that the source system's data is GMP controlled, including its reliability.	
Data processing Def. - A sequence of operations performed on data to extract, present, or obtain information in a defined format (14).	• Validate systems performing GMP functions for their intended use, with particular attention to data operation, performance, and management. Some examples of functionality performed by systems are archiving, audit trails, e-signatures, operational checks, printouts/reports, security, and so on.	

Table 1- Data Integrity By Design

If electronic systems are utilized to produce e-records or shared drive (19) to store e-records required under GMPs, these systems should include (but is not limited to) the following elements:

- Validate electronic systems and qualify repositories for e-records (20) for their intended use, with particular attention to any user to produce and store data, correspondingly.
- Ensure all access and user rights in electronic systems and shared drives are adequately controlled to prevent system users from compromising e-records integrity.
- Control e-records in a way that ensures that the e-records:
    a. can only be created and modified by authorized automated system/personnel.
    b. are protected against intentional or accidental deletion.
    c. are named and organized in a way that allows for easy traceability.
    d. are tracked through an audit trail when modified (the audit trail should include changes made to the record, who made the change, the time and date the record was changed and, if applicable, the reason the record was modified).
    e. are backed up at regular intervals to protect against potential data loss due to system issues or data corruption.
    f. are available for review during an inspection and are readily retrievable in a suitable format; and
    g. include all necessary metadata.

SUMMARY

The data integrity strategy's foundation originates in the GDPs that can be found in the GMPs.

The expectations and supporting controls listed in Table 1 are performed throughout the data retention period and are the essential elements of data integrity applicable to paper records.

The requirements for record integrity do not differ depending on the data format; paper and electronic-based systems. Both systems are subject to the exact requirements.

The e-records data integrity controls listed in this article summarize the same listed control applicable to paper records.

REFERENCES

1. A global abbreviation intended to cover the context of GMP, GCP, GLP, and other regulated applications. The underlying international life science requirements are those outlined in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese MHL.W regulations, Australia TGA, or other applicable national legislation or regulations under which a company operates. (GAMP Good Practice Guide, IT Infrastructure Control and Compliance, ISPE 2005)
2. Data is defined as the content of a record. It is the basic unit of information with a unique meaning and can be transmitted. (ISO/IEC 17025)
3. Data integrity - The property that the data is complete has not been altered in an unauthorized manner. When altered in an authorized manner, the alteration is traceable to the original data. Data integrity covers data

entry or collection, storage, transmission, and processing. Completeness is the property that all necessary parts of the entity in question are included (NIST SP 800-57P1)

4. Data consistency refers to whether the same data kept at different places do or do not match.
5. https://www.trifacta.com/what-is-data-integrity/
6. Regulated entity - the regulated Good Practice company responsible for the operation of an electronic system and the applications, files and data held thereon.
7. Good Practice for Data Management and Integrity in Regulated GMP/GDP Environments – PIC/S; PI041-1; July 2021. PIC_S PI 041-1.
8. Regulated users - the group responsible for operating a system. (GAMP)
9. Electronic systems mean systems, including hardware and software, that produce electronic records. (DoD)
10. Records are a collection of related data treated as a unit. (ISPE/PDA, "Good Practice and Compliance for Electronic Records and Signatures. Part 1 Good Electronic Records Management (GERM)". July 2002)
11. OECD, Advisory Document of the Working Party on GLP on GLP Data Integrity, September 2021 (Final)
12. López, O., "*A Computer Data Integrity Compliance Model*," Pharmaceutical Engineering 35, No 2 (March/April 2015); 79-87.
13. Sensor data is the output of a device that detects and responds to some input from the physical environment.
14. NARA, "*Universal ERM Requirements*," Version 2.03.
15. Data accuracy refers to whether the data values stored for an object are the correct values.
16. True copy - An exact copy of an original record, which may be retained in the same or different format in which it was initially generated, e.g., a paper copy of a paper record, an electronic scan of a paper record, or a paper record of electronically generated data. (MHRA)
17. A reliable record is one whose content can be trusted as a complete and accurate representation of the transactions, activities, or facts to which they attest and can be depended upon in the course of subsequent transactions or activities (NARA). Complete is the property that includes all necessary parts of the entity in question. Accurate data refers to whether the data values stored for an object are correct.
18. MHRA, "*GxP Data Integrity Guidance and Definitions*," March 2018.
19. Shared Drives, also known as network drives, refer to managed shared servers that provide electronic storage space for authorized users to house e-records in supported file formats. Shared Drives can be managed on-premises or in the cloud. An example of a shared drive in the cloud is Data as a Service (DaaS).
20. Repositories for e-records are direct access devices on which the electronic records and metadata are stored.

ADDITIONAL READINGS

1. López, O., "*Ensuring the Integrity of Electronic Health Records*," Routledge, Boca Ratón, Fl., 2021.
2. López, O., "*Data Integrity in Pharmaceutical and Medical Devices Regulation Operations: Best Practices Guide to Electronic Records Compliance*," CRC Press, Boca Ratón, Fl., 2017.