MHRA Data Integrity Guidance: Implementation Approach

By Ivan Soto  May 30, 2017 4:22 pm EDT

Introduction

In March 2015, the U.K. Medicines and Healthcare Products Regulatory Agency (MHRA) published “GMP Data Integrity Definitions and Guidance.” This document outlines the definitions, principles, requirements, and approaches that MHRA considers appropriate aspects of data integrity.

Since 2015 the industry has struggled with compliance and implementation of this data integrity guidance document. During MHRA inspections, several data integrity deficiencies have been found that lead to regulatory observations.

Unfortunately, companies have failed to define an implementation strategy that enables alignment with this data integrity guidance document.

The lack of an implementation strategy is mostly due to the lack of understanding with data integrity requirements found in the MHRA guidance document.

This article will provide clarity and understanding of the data integrity requirements found in the guidance document. This article will also provide implementation strategy approaches to promote alignment and compliance with the data integrity requirements found in this guidance document.

General Requirements

Data integrity is considered a fundamental aspect of the quality system. MHRA clearly communicates the requirement of defining data governance as an integral part of the pharmaceutical quality system.

This guidance document doesn’t define any expectations to the industry to implement a forensic approach to data verification. MHRA expectations is that data governance should be designed and operate in a state of control based on the data integrity risk.

This guidance document clearly communicates the expectation that data integrity risk is formally assessed and documented in a formally approved risk assessment to support all decisions and rationale.

Data integrity applies to both paper and electronic systems. Eliminating electronic systems and reverting to paper will not itself remove the need to implement data integrity controls.

Defining Data Integrity Risk & Criticality
The data governance system needs to include relevant policies, standards, and procedures. It also needs to include training on the importance of data integrity. In addition, training will need to provide data integrity policies, standards and procedures.

Data governance must address and define data ownership throughout the data's lifecycle. Data governance must have the design, operation, and monitoring of systems and processes. Some of these processes include logical security, audit trails, intrusion detection mechanisms, alerts, and controls over intentional and unintentional changes to data and information.

The amount of effort and controls applied during the data lifecycle should be based on criticality and risk based on the impact on critical quality attributes.

The risk to data integrity is based on the complexity of the system, ability to manipulate data, patient safety, impact to critical parameters, and product quality attributes.

To understand the risk and criticality of data, companies should perform a risk assessment. The risk assessment is intended to identify the risk factor of the data and identify whether the data is high, medium or low risk.

The results of the risk should be used to define the data integrity implementation strategy which are comprised of technical and procedure controls.

The rationale for this approach is based on the fact that not all data has the same level of criticality and risk impact. Implementing a one-size-fits-all approach for data integrity is not an adequate scalable solution.

A risk-based approach to data governance and data integrity ensures that critical high risk data is managed and controlled adequately and is based on its impact to critical process parameters and related product quality attributes.

**Expectations for Data Integrity & Quality**

Compliance with current data integrity expectations requires an understanding of all the requirements defined in the MHRA guidance document.

One of the main expectations is that data must be:

- **A** – attributable to the person generating data
- **L** – legible and permanent
- **C** – contemporaneous
- **O** – original record
- **A** – accurate

Several articles and presentations have been published in industry journals about the ALCOA concept. Unfortunately, most of these articles mostly describe the philosophies of these concepts and fail to provide strategic direction for implementing the concepts.

**Attributable:** For data to be attributable, companies need to implement technical and procedure controls to ensure that the data is accurately associated with the person generating the data. Procedures need to be concise and accurate, while containing directions and actions to ensure that data is attributable to the person generating the data.
Legible and permanent: Legible and permanent data is a predicate rule found under the Good Documentation Practices regulatory requirements (Medicines & Healthcare Products Regulatory Agency, 2015, p. 4).

Procedures need to describe the necessary requirements to ensure that data is legible and permanent during its lifecycle, which is a critical data integrity requirement.

Contemporaneous: Technical and procedure controls need to clearly describe the requirements for data to be contemporaneous. These controls need to ensure that data originates during the same time that it’s generated. This ensures data integrity and reduces the risk of losing, falsifying, or manipulating data. For electronic systems, technical controls need to be implemented to ensure that data is contemporaneous. For paper-based processes, procedure controls need to be in place to ensure that all data generated manually is contemporaneous. Computer systems are expected to be designed to ensure that the execution of critical operations are recorded contemporaneously by the user. Computer systems’ critical operations are expected to not be combined with other operations.

Original: Data integrity expectations require data to be original. Original data must come from the source or condition where the data was generated. Electronic systems need to have adequate design and technical controls that ensure that all data generated electronically is original. These technical controls need to include logic and functionality that records the original data at the initial point of generation, including a date and time stamp. Paper-based, manually generated data procedures need to have adequate controls to ensure that data is original and accurate.

Permanent: Raw data - whether found in electronic systems or on paper - needs to be legible and accessible during its lifecycle. Data integrity expectations require that raw data must be able to allow full reconstruction of the activity resulting in data generation.

For paper-based data and records, these expectations require companies to ensure the preservation of data and its chronology during its lifecycle. This requires adequate document archival and storage control to ensure that data is legible during its lifecycle. In addition to document storage controls, companies need to ensure that all paper-based data is related to a specific GMP system. Also, the activity must be linked together using databases or tracking mechanisms that facilitate full reconstruction of the activity generating the data.

Accurate: Systems must be designed in way that ensures data integrity, quality, and compliance.

The following design controls are considered critical and should be implemented to ensure data integrity and compliance:

- Access to accurate clocks to record time events
- Accessibility to batch records near the location where activities are taking place
- Adequate controls over blank paper templates for data recording
- User access rights which prevent data manipulation
- Audit trails to detect data integrity issues
- Automated real-time data capture or printers attached to equipment
- Proximity of output devices (e.g printers) to relevant activities
• Easy and close access to raw data for staff performing data verification activities

These design control expectations include both electronic and paper records used in the pharmaceutical industry.

Electronic systems used to generate GMP data needs to be designed with adequate audit trails, and include retention of the entire audit trail to show all changes to the data throughout its lifecycle. Audit trails must be designed to enable the ability to associate all data changes with the individuals performing those changes and with a date and time stamp. Electronic systems must be designed to disable the ability to change, manipulate, delete or switch-off the audit trails.

The information retained in the audit trails should be used by companies to ensure robust data review and verification. The expectation is that audit trail reviews must be performed during the routine data review and verification process. Routine audit trail reviews must be documented and available during inspections to provide evidence of compliance with this requirement. The implementation of audit trails reviews must be based on the risk of the data and its impact to critical quality attributes. It is highly recommended that companies take a risk-based approach when implementing audit trail reviews. Failure to follow a risk-based approach may lead companies to implement audit trail reviews for all data which is not scalable and sustainable in the long term.

Systems that do not provide an electronic audit trail must have a paper-audit trail for changes to GMP data.

Approved procedures must be in place to describe the process for data reviews and include the actions to be taken when issues are found. Data reviews must include all relevant data including metadata and audit trails.

**Limited Access**

Computer systems must be designed with an access controls mechanism to ensure that users have access only to functionality that is appropriate to their job role. To ensure data integrity, sharing passwords and generic user ID’s are not permitted under the expectations defined by MHRA in their guidance document.

Companies are expected to upgrade all legacy systems by the end of 2017 that do not enable unique user ID’s and passwords

System administrator access must be restricted to the minimum number of people possible. All generic system administration accounts must be disabled or changed to become traceable to a single administrator.

**Retention**

Data integrity requires controls that ensure adequate record retention. Raw data found in paper can be retained by scanning the record. Scanned paper records need to be have a verification to ensure the completeness, accuracy and integrity of the data. Data and document retention must have controls in place to ensure that there is no data alteration or loss.
Validation

All GMP computer systems must be validated for their intended purpose. The expectation is that companies during validation have an understanding of electronic system function within a process. Companies are expected to validate their specific configuration and intended use based on their business process. Vendor validation documentation is not considered acceptable to provide evidence that the company intended use and unique configuration are validated.

Implementation Strategies

Companies need to develop implementation strategies that enable complete alignment with the MHRA Data Integrity guidance document.

To enable complete alignment companies, need to understand their current status against the MHRA data integrity requirements. In order to understand the current status companies, need to perform gap assessments to identify the areas that are not in compliance and complete alignment with the MHRA data integrity requirements. To perform this activity companies, need to create a gap assessment tool to identify all the areas that need alignment. The gap assessment tool should list all the MHRA data integrity requirements and identify all areas of alignment and gaps.

To close all the gaps companies, need to create remediation plans that describe all the activities needed to close all the data integrity gaps. CAPA’s need to be created to describe and track all the corrective actions.

Once all CAPA’s are closed and remediation activities complete a remediation summary report should be created to summarize all corrective action activities.

Performing the gap assessments, creating the remediation plans, CAPA’s and summary report provides a structured approach that ensures complete alignment with MHRA data integrity requirements.

Summary

MHRA data integrity requirements require companies to implement technical and procedure controls. Data integrity applies to both paper and electronic records.

Most companies are not in alignment with MHRA data integrity requirements. Companies often times fail to implement an adequate strategy that enable complete alignment with data integrity requirements.

In order to enable alignment with data integrity requirements companies must perform gap assessments to identify areas that need corrective actions.

Performing documented gap assessments, creating remediation plans and CAPA’s provides a structured approach to identify gaps, and corrective actions that enable complete alignment with MHRA data integrity requirements.

Reference:
Source URL: http://www.ivtnetwork.com/article/mhra-data-integrity-guidance-implementation-approach