Review of Good Data Integrity Principles

Covering the recent emphasis on data integrity by regulatory agencies, currently existing data integrity guidelines, and who data integrity guidelines most affect

Ofni Systems

808 Salem Woods Drive Suite 103
Raleigh, NC 27615
(919) 844-2494

Table of Contents

Introduction and Sources of Information

What is Data Integrity?

Data integrity is the idea of maintaining and ensuring the accuracy and consistency of data over its lifecycle. This includes good data management practices, such as preventing data from being altered each time it is copied or moved. Data integrity applies to both paper records and electronic records. Processes and procedures are put in place for companies to maintain data integrity during normal operation [1].

Data Integrity Importance

Data in its final state is the driving force behind industry decision making. Raw data must be changed and processed to reach a more usable format. Data integrity ensures that this data is attributable, legible, contemporaneous, original, and accurate (ALCOA). Data can easily become compromised if proper measures are not taken to ensure data safety. Errors with data integrity commonly rise from human error, noncompliant operating procedures, data transfers, software defects, compromised hardware, and physical compromise to devices. Maintaining data integrity is a necessary part of the industry’s responsibility to ensure the safety, effectiveness, and quality of their products [1].

Principles of ALCOA

In recent years, regulators have found that many organizations are falling short when it comes to maintaining adequate data integrity within computerized systems. Due to the increasing number of observations related to data integrity made during inspections, a WHO committee has decided to outline a new guidance meant to consolidate and improve upon existing principles ensuring data integrity from current good practices and guidance documents [2].

ALCOA Defined

Attributable: Every piece of data entered into the record must be capable of being traced back to the time it was taken and to the individual who entered it.

Legible: All data (including metadata) must be traceable, permanent, readable, and understandable by anyone reviewing the record.

Contemporaneous: Data that are summarily entered into the record at the time they are generated.

Original: Source data that is the record medium in which the data was first recorded. An original data record should include the first data entered and all successive data entries required to fully detail the scope of the project.

Accurate: Correct, truthful, complete, valid, and reliable data with controls in place to assure the accuracy of data should be implemented on a risk-based structure [2].

Meeting ALCOA Data Expectations

Attributable: Requires the use of secure and unique user logons and electronic signatures. Using generic login IDs or sharing credentials must always be avoided. Unique user logons allow for individuals to be linked to the creation, modification, or deletion of data within the record. For a signature to be legally-binding there should be a secure link between the person signing and the resulting signature. The use of digital images of hand written signatures is not considered a secure or credible method for electronically signing documents [2].

Legible: In order for an electronic record to be considered legible, traceable, and permanent it must utilize controls such as following SOPs and designing a system that promotes saving electronic data in concurrence with the execution of the activity. This is best done by prohibiting the creation of data in temporary memory as well as immediately committing data to a permanent memory before moving on. Secure time stamped audit trails are to be used to record operator actions. The system configuration must limit security rights allowing users to turn off the audit trail or overwrite data. These administrative rights should be reserved (whenever possible) for individuals who are independent of those responsible for the content of the electronic records. Improperly overwriting data or manipulating the audit trail impairs the legibility of the data by obscuring the original value of the record [2].

Contemporaneous: Utilizes the controls of writing SOPs and maintaining settings that immediately commit data to a permanent memory. In order for the data to be considered contemporaneous, the record must also have a secure time stamp system that cannot be altered by users. Time and date stamps need to be synchronized across all systems involved in the GxP activity. Data is not considered contemporaneous when recorded on an unofficial document and then later entered into the official electronic record [2].

Original: Original electronic records (or certified true copies) must be reviewed and approved with standardized procedures. These procedures should describe the review method itself as well as any changes made to the information in the original records, including changes documented in audit trails or any other relevant metadata. Written procedures should define the frequency, roles and responsibilities, and approach to the review of metadata. Once reviewed, electronic data sets should be electronically signed to document their approval. Controls should also be put in place to guarantee the retention of original electronic documents as best as possible. The original record should be routinely backed up and stored separately in a safe location in case the original record is lost. Secure storage areas should have a designated electronic archivist who is independent of the GxP operation. Tests ought to be carried out at times in order to verify that the copy can be retrieved and utilized from secure storage areas [2].

Accurate: Data should be maintained through a quality management system that is risk-based. Routine calibration and equipment maintenance needs to be performed. Computer systems that generate, maintain, distribute, or archive electronic records should be validated. Entry of critical data such as high priority formulas for spreadsheets should be verified by two authorized individuals. Once verified, critical data fields must be locked to prevent modification by any unauthorized individuals [2].

Data Integrity Guidance Documents

As the pharmaceutical and medical device industries continue to grow and outsource work, an increasing number of guidance documents are released to regulate and supervise production and development. In July 2012, the Food and Drug Administration (FDA) Safety and Innovation Act was signed into law. FDASIA increases the FDA's authority to have better control over the increasing global drug supply chain. Nearly 80 percent of active ingredients for pharmaceuticals comes from sources overseas [3]. Due to this increasing market, the foreign drug quality inspections nearly doubled from 2010 to 2015.

The FDA responded with guidance intended to improve data integrity in Clinical Investigations as well as draft guidance to address more recent questions and concerns on data integrity for GMP facilities. The World Health Organization (WHO) released Annex 5 Guidance on Good Data and Record Management Practices, a guidance to help bridge the gaps in current data integrity guidance. The Medicines and Healthcare products Regulatory Agency (MHRA) released draft guidance to address similar data integrity topics as compared to the FDA's draft guidance. The FDA's draft guidance is aimed towards GMP facilities where the MHRA's guidance is aimed towards GxP facilities.

FDA Draft Guidance on Data Integrity

In April 2016, the FDA issued draft guidance for industry on data integrity and compliance with cGMP [4]. This new guidance was released in response to a recent influx in data manipulation concerns. The purpose of this new draft guidance is to ensure data integrity in the pharmaceutical industry through sharing the FDA's current thoughts on the creation and handling of data. The draft guidelines, which are formatted as a question and answer format, provide the industry with suggestions on how to meet data integrity standards and supplemental information on cGMP terminology.

The FDA proposes that audit trails be reviewed with each record and before the final approval of a record. The contents of the audit trail that need to be reviewed include the change history of finished product test results, changes to sample run sequences, changes to sample identification and changes to critical process parameters.

Other key points from the draft guidance include the following:

- What systems need to be validated?
- How should access to computer systems be controlled and monitored?
- When should audit trails be reviewed and who should review them?
- What are the differences between static and dynamic records?
- What training is necessary for personnel regarding detection of data integrity issues?
- How do you address data integrity problems that are identified by the FDA? [4]

FDA Guidance on Electronic Source Data in Clinical Investigations

In September 2013, the FDA published guidance for sponsors, Contract Research Organizations (CROs), clinical investigators, and others involved with FDA regulated clinical investigation source data. This guidance is intended to help ensure that data from electronic sources is reliable, of quality and integrity, and is traceable. The source data used to fill electronic case report forms (eCRFs) is one of the main topics covered by this guidance [5].

WHO Guidance on Good Data and Record Management Practices

The World Health Organization (WHO) is an agency of the United Nations concerned with international public health. In 2016 the WHO Expert Committee on Specifications for Pharmaceutical Preparations released guidance on good data and record management practices (Annex 5) discussing the following relevant topics:

- ALCOA
- Quality risk management
- Good data and documentation practices
- Design and validation of systems to ensure data quality and reliability
- Addressing data reliability issues [2]

MHRA GxP Data Integrity Definitions and Guidance for Industry

The MHRA is responsible for ensuring that pharmaceuticals and medical devices are appropriately regulated for safety and functionality in the United Kingdom. In July 2016 the MHRA released draft guidance on data integrity which includes definitions and guidance for industry. The guidance covers the importance of designing systems that encourage good data integrity practices and tips for designing these systems. In the draft guidance, the MHRA proposes that GMP facilities should upgrade to an audit trailed system if their paper based or hybrid systems cannot demonstrate equivalence to a fully automated audit trail. The MHRA also proposes that GMP facilities upgrade to computer systems that allow for each user to have an individual login with audit trails. It is proposed that both of these changes be made by the end of 2017 [6].

Data Integrity Training and Auditing

Data Alteration Controls

One of the most common violations cited in FDA inspections is the lack of controls to prevent changes to electronic records. Having common users with permissions to delete or change data is a huge red flag for FDA inspectors. This is especially the case when those users all share a common logon ID or have the ability to deactivate the audit trail. Sharing user logon IDs automatically disqualifies data from being considered attributable and therefore the data is no longer ALCOA compliant. Furthermore, the lack of a secure audit trail violates almost every aspect of ALCOA data integrity practices [2].

> Ofni Systems' ExcelSafe is used to control and monitor changes made to spreadsheets. It has an audit trail function that tracks all changes made to a spreadsheet. The audit trails are secure and cannot be disabled. ExcelSafe provides users with unique logon IDs and passwords allowing for the audit trail to distinguish between personnel. Users are given specific permissions to ensure that only those with authorization can alter data in the spreadsheet.

Assigning Roles and Providing Appropriate Training

An essential step to prevent data integrity violations is to ensure that every user has a unique logon ID and password. Users are to be trained to never share their passwords under any circumstances. Computer or application locking procedures should be implemented to prevent unauthorized use. Each user should only be given permissions appropriate to their role (i.e. read only users, data entry personnel, and system administrators) and should receive a level of training corresponding to their role. Data audit trails must be secure and record every change made to the record including the user who made the change and the exact time and date the change was made [2].

Auditing roles should be assigned to personnel who have been trained in performing audits. The properly trained personnel are expected to routinely audit company procedures and records in order to search for data integrity issues. Auditors should audit records they are uninvolved with in order to prevent bias.

> If your company does not have personnel trained to perform internal audits, Ofni Systems can act as an unbiased third party auditor to ensure that your facilities are GxP compliant and are following good data integrity guidelines.

When assigning roles it is important to consider how each individual will have to act when the site is audited by the FDA. In particular, the system administrator role should be considered as more than a technical position. During an FDA audit, the administrator will be required to demonstrate the system and to answer detailed questions about audit trails, security features, and system configuration options. This person must be capable of appearing confident and professional under the pressure of a data integrity audit [1]. To prevent conflicts of interest, system administrators should be carefully chosen individuals who are not biased towards the content of the record [2].

Data Integrity Training Procedures

Personnel should be effectively trained on detecting data integrity issues and implementing good data integrity practices. Standard operating procedures (SOPs) should be clearly written and regularly implemented. There needs to be training documentation stating that each individual has read the SOPs and understands them. The SOPs should include instructions such as personnel responsible for recording data, what type of data and metadata should be recorded, and how to record data. Individuals should also be trained on the importance of maintaining accurate and complete audit trails to prove data integrity.

Analytical Laboratories

Results from analytical laboratories are used to make decisions in the pharmaceutical industry on materials and processes involved in creating products used by patients. Since the final manufactured products are based on results from analytical laboratories, adhering to strict data integrity standards is essential. All results and laboratory records need to be retained for review by the FDA [4].

When the FDA audits analytical laboratories, there are several issues that come up most frequently which could compromise data integrity. In laboratories each employee must have unique logon credentials and personnel should never share passwords. When passwords are shared or nonexistent it becomes impossible to correctly identify which user made changes to a record. User privileges should be segregated depending on an individual's roles and training. Proper computer system control should be in place including the prevention of modification or deletion of electronic files. This requirement is in place to ensure that electronic records maintain their integrity. Procedures for data integration must be in place and integration parameters must be controlled. Data must be complete, including all raw data, graphs, charts, and spectra from laboratory instruments. All data and equipment are to be properly identified. Audit trail functionality should not be turned off. The presence of a complete and accurate audit trail is necessary to maintain data integrity because it shows when a record was modified, who modified the record and where the data came from [1].

In analytical laboratories it is crucial to have clearly written procedures for each analytical technique and laboratory operation performed. To clarify procedures, a technique called process flow mapping can be used. Process flow mapping connects all aspects of a process and is helpful to reference, especially during internal audits. Mapping out a process will help identify where any data integrity issues may have originated from and who caused them. Process flow mapping should identify the actions that are performed, a step by step procedure for performing each action, the associated risk, methods for preventing or detecting fraud, methods for recording data and making decisions, and the individual responsible for each process step [1].

Medical Devices

Since design decisions for medical devices are made based on study data, data integrity is necessary in the medical device industry. It is recommended by the Parental Drug Association (PDA) that medical device companies perform internal audits at least once every three years, unless the device is considered high risk, in which case audits should be more frequent. Audits should be internally carried out unannounced and be especially focused on higher risk areas for the medical device. Auditors may also visit manufacturer's subcontractors or suppliers to ensure data integrity is being maintained in these locations. When auditing medical devices, auditors look for the following:

Device description
Device intended use
Device classification
Device labelling
Harmonized standards compliance
Complaint/vigilance evaluation
Risk assessment
Pre-clinical testing
Stability
Biocompatibility
Sterilization
Clinical evaluation [7]

When auditing medical devices, auditors encounter common data integrity issues such as the inability to trace the path of a specific device component throughout its life cycle. In order to ensure that auditors do not find fault with your medical device documentation, verify the following:

- All documentation related to the compliance assessment of the device is accounted for.
- The technical documentation is accurate, consistent, completed, and updated.
- All documentation can be 100% attributed to the specific device being audited.

- All materials and parts of the medical device have the necessary records so they can be traced throughout their life cycles [7].

Clinical Investigations

The data integrity clinical investigation guidelines are important for clinical study sponsors, CROs, and clinical investigators to abide by due to the nature of the data they are collecting. Clinical study source data, which includes information in original records and certified copies of original records, should be ALCOA and meet recordkeeping regulatory requirements. Source data can be entered into an electronic case report form (eCRF), which is an auditable electronic record presented to the sponsor for each trial subject [5].

Electronic Source Data Overview

A list of data originators must be developed by the sponsor and kept on all clinical study sites. All individuals will be assigned their own logon information, and only individuals with authorization should be able to access eCRF data. If a study individual becomes inactive, their logon access needs to be disabled. Depending on the situation, the data originator can be defined as the clinical investigator, the clinical investigation subjects, medical devices, electronic health records, automated lab reporting equipment, and other technologies. Each element of data should have its own identifier that is automatically populated into the corresponding data field in the eCRF to facilitate audit trail review [5].

eCRF Data Capturing

Data element identifiers (including the data originators, the date and time the data was entered, and the clinical investigation subjects to which the data corresponds) should be populated automatically into the appropriate field in the eCRF. If any changes are made to data, the previous identifier must not be obscured and a reason for change must be provided. It is recommended that eCRFs include checks in order to minimize data integrity issues such as missing data or out of spec values. After clinical investigators perform data reviews, they electronically sign completed eCRFs before archiving data or submitting them to the FDA in order to satisfy 21 CFR Part 11 requirements (the EHRs themselves do not need to be Part 11 compliant) [5].

Good Manufacturing Practices

For pharmaceutical manufacturers and medical device manufacturers, maintaining data integrity is of great importance. The FDA takes incomplete records and faulty documentation to be a sign that the entire operation is out of control and the final product cannot be considered quality. Maintaining good documentation is just as important as maintaining clean facilities and creating safe and effective products. Documentation in a pharmaceutical facility includes both paper records and electronic records. This includes but is not limited to adverse events reports, complaints, batch records, and quality systems. These records must provide the necessary proof that the product being manufactured is stable, sterile, and biocompatible. Documentation must also enable tracking of each component of the manufactured product or batch from the beginning to the end of its lifecycle to provide the traceability necessary in case there are issues with a specific component.

Audit Trail Summary Tools

The FDA has increased requirements on audit trail review. Audit trails generated by computer systems are time consuming and tedious to review. The FDA's proposed requirements increase workload dramatically, leaving QA with the daunting task of sorting through hundreds or even thousands of records.

When performing a quality audit, one would manually search the audit trail for:

- Additions, edits, and deletions of records, data, formulas, etc.
- Contributors and electronic signatures
- Reasons for change
- Verification of data integrity
- Identifiers such as workstation name, windows login ID, IP address
- Configuration settings
- Original or resampled data and test results
- Time and date stamps for changes made and sequence of events

Reviewing the audit trails is not only a proposed requirement by the FDA; it is also beneficial to the company itself. By catching data integrity issues early, risks to the company are reduced. It can help identify issues with data collection and processes sooner than they would otherwise be uncovered.

One proposed solution to speeding up the audit trail review process is to let the software that created the electronic audit trail provide assistance in summarizing that same audit trail for the user. This would essentially perform the majority of the manual QA review task. Software is better at searching, sorting, and filtering large datasets than humans. The data integrity issues that QA professionals look for can be easily coded and presented for review.

Ofni Systems has developed an audit trail summary tool for reviewing audit trails that will drastically lighten the workload to perform a quality audit. The summary tool filters through audit trails and finds every entry. The tool can categorize data by the contributor, the types of changes made to data, the date/time of data entry, and more. The audit trail summary tool is configurable to meet your needs. Due to common mistakes being flagged, the summary tool allows for more data integrity issues to be identified. The audit trail summary tool is adaptable to a wide variety of audit trails and will enable its users to satisfy the FDA requirements for audit trail review.

References

To see examples of data integrity issues caught by the FDA, read through some of the recently issued warning letters.

[1] Smith, P. (2014, May 2). Data Integrity in the Analytical Laboratory. Retrieved from http://www.pharmtech.com/data-integrity-analytical-laboratory

[2] World Health Organization. (2016). Guidance on good data and record management practices. Retrieved from http://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf

[3] Food and Drug Administration. (2016, October 6). Food and Drug Administration Safety and Innovation Act (FDASIA). Retrieved from http://www.fda.gov/RegulatoryInformation/Legislation/SignificantAmendmentstotheFDCAct/FDASIA/ucm20027187.htm

[4] Food and Drug Administration. (2016, April). Data Integrity and Compliance with CGMP Guidance for Industry. Retrieved from http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm495891.pdf

[5] Food and Drug Administration. (2013, September). Guidance for Industry Electronic Source Data in Clinical Investigations. Retrieved from http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm328691.pdf

[6] MHRA. (2016, July). MHRA GxP Data Integrity Definitions and Guidance for Industry. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf

[7] Parental Drug Association. (2015, May 12). Data Integrity Seminar Presentation. Retrieved from https://www.pda.org/docs/default-source/website-document-library/chapters/presentations/ireland/pda-data-integrity-seminar-presentations.pdf?sfvrsn=4