



DATA INTEGRITY: A NEED OF PHARMACEUTICAL INDUSTRY

^{*1}Shivani S. Ingawale, ²Avinash M. Bhagwat, ³Anand P. Khadke and ⁴Anuradha A. khadke

¹Student, Yashoda Technical Campus Satara Faculty of Pharmacy.

²Assistant Professor, Pharmaceutical Analysis Yashoda Technical Campus Satara Faculty of Pharmacy.

³Assistant Professor, Pharmaceutical Chemistry Yashoda Technical Campus Satara Faculty of Pharmacy.

⁴JSPM's Jayawantrao Sawant College of Pharmacy.

***Corresponding Author: Shivani S. Ingawale**

Student, Yashoda Technical Campus Satara Faculty of Pharmacy.

Article Received on 07/03/2017

Article Revised on 27/03/2017

Article Accepted on 17/04/2017

ABSTRACT

Data integrity ensures that this data is attributable, legible, contemporaneous, original, and accurate (ALCOA). Maintaining data integrity is a necessary part of the industry's responsibility to ensure the safety, effectiveness and quality of their products. is critically important in the pharmaceutical industry. The extent of Management's knowledge and understanding of data integrity can influence the organisation's success of data integrity management. Management must know their legal and moral obligation (i.e., duty and power) to prevent data integrity lapses from occurring and to detect them, if they should occur. This review contains its types, principles, varies important guidance and issues, warring latters, preventions of data integrity issues, audit trials etc.

KEYWORDS: Data integrity preventions of data integrity issues, audit trials etc.

INTRODUCTION

Data Integrity

Data integrity is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle.^[1] and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. The term *data integrity* is broad in scope and may have widely different meanings depending on the specific context – even under the same general umbrella of computing. This article provides only a broad overview of some of the different types and concerns of data integrity.

For the purposes of this guidance, data integrity refers to the completeness, consistency and accuracy of data. Complete, consistent and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy and accurate (ALCOA).^[2]

Data integrity is the opposite of data corruption, which is a form of data loss. The overall intent of any data integrity technique is the same: ensure data is recorded exactly as intended and upon later retrieval, ensure the data is the same as it was when it was originally recorded. In short, data integrity aims to prevent unintentional changes to information. Data integrity is not to be confused with data security, the discipline of protecting data from unauthorized parties. Any unintended changes to data as the result of a storage, retrieval or processing operation, including malicious

intent, unexpected hardware failure, and human error, is failure of data integrity. If the changes are the result of unauthorized access, it may also be a failure of data security. Depending on the data involved this could manifest itself as benign as a single pixel in an image appearing a different color than was originally recorded, to the loss of vacation pictures or a business-critical database, to even catastrophic loss of human life in a life-critical system.

integrity types

- Physical integrity
- Logical integrity

Physical integrity

Physical integrity deals with challenges associated with correctly storing and fetching the data itself. Challenges with physical integrity may include electromechanical faults, design flaws, material fatigue, corrosion, power outages, natural disasters, acts of war and terrorism and other special environmental hazards such as ionizing radiation, extreme temperatures, pressures and g-forces. Ensuring physical integrity includes methods such as redundant hardware, an uninterruptible power supply, certain types of RAID arrays, radiation hardened chips, error-correcting memory, use of a clustered file system, using file systems that employ block level checksums such as ZFS, storage arrays that compute parity calculations such as exclusive or or use

a cryptographic hash function and even having a watchdog timer on critical subsystems.

Logical integrity

This type of integrity is concerned with the correctness or rationality of a piece of data, given a particular context. This includes topics such as referential integrity and entity integrity in a relational database or correctly ignoring impossible sensor data in robotic systems. These concerns involve ensuring that the data "makes sense" given its environment. Challenges include software bugs, design flaws and human errors. Common methods of ensuring logical integrity include things such as a check constraints, foreign key constraints, program assertions and other run-time sanity checks.

Both physical and logical integrity often share many common challenges such as human errors and design flaws, and both must appropriately deal with concurrent requests to record and retrieve data, the latter of which is entirely a subject on its own.

Databases

Data integrity contains guidelines for data retention, specifying or guaranteeing the length of time data can be retained in a particular database. It specifies what can be done with data values when their validity or usefulness expires. In order to achieve data integrity, these rules are consistently and routinely applied to all data entering the system, and any relaxation of enforcement could cause errors in the data. Implementing checks on the data as close as possible to the source of input (such as human data entry), causes less erroneous data to enter the system. Strict enforcement of data integrity rules causes the error rates to be lower, resulting in time saved troubleshooting and tracing erroneous data and the errors it causes algorithms. Data integrity also includes rules defining the relations a piece of data can have, to other pieces of data, such as a *Customer* record being allowed to link to purchased *Products*, but not to unrelated data such as *Corporate Assets*. Data integrity often includes checks and correction for invalid data, based on a fixed schema or a predefined set of rules. An example being textual data entered where a date-time value is required. Rules for data derivation are also applicable, specifying how a data value is derived based on algorithm, contributors and conditions. It also specifies the conditions on how the data value could be re-derived.

Types of integrity constraints

Data integrity is normally enforced in a database system by a series of integrity constraints or rules. Three types of integrity constraints are an inherent part of the relational data model: entity integrity, referential integrity and domain integrity:

- Entity integrity concerns the concept of a primary key. Entity integrity is an integrity rule which states that every table must have a primary key and that the

column or columns chosen to be the primary key should be unique and not null.

- Referential integrity concerns the concept of a foreign key. The referential integrity rule states that any foreign-key value can only be in one of two states. The usual state of affairs is that the foreign-key value refers to a primary key value of some table in the database. Occasionally, and this will depend on the rules of the data owner, a foreign-key value can be null. In this case we are explicitly saying that either there is no relationship between the objects represented in the database or that this relationship is unknown.
- *Domain integrity* specifies that all columns in a relational database must be declared upon a defined domain. The primary unit of data in the relational data model is the data item. Such data items are said to be non-decomposable or atomic. A domain is a set of values of the same type. Domains are therefore pools of values from which actual values appearing in the columns of a table are drawn.
- *User-defined integrity* refers to a set of rules specified by a user, which do not belong to the entity, domain and referential integrity categories.

If a database supports these features, it is the responsibility of the database to ensure data integrity as well as the consistency model for the data storage and retrieval. If a database does not support these features it is the responsibility of the applications to ensure data integrity while the database supports the consistency model for the data storage and retrieval.

Having a single, well-controlled, and well-defined data-integrity system increases

- stability (one centralized system performs all data integrity operations)
- performance (all data integrity operations are performed in the same tier as the consistency model)
- re-usability (all applications benefit from a single centralized data integrity system)
- maintainability (one centralized system for all data integrity administration).

As of 2012, since all modern databases support these features (see Comparison of relational database management systems), it has become the de facto responsibility of the database to ensure data integrity. Out-dated and legacy systems that use file systems (text, spreadsheets, ISAM, flat files, etc.) for their consistency model lack any kind of data-integrity model. This requires organizations to invest a large amount of time, money and personnel in building data-integrity systems on a per-application basis that needlessly duplicate the existing data integrity systems found in modern databases. Many companies and indeed many database systems themselves, offer products and services to migrate out-dated and legacy systems to modern databases to provide these data-integrity features. This offers organizations substantial savings in time, money

and resources because they do not have to develop per-application data-integrity systems that must be refactored each time the business requirements change.

Examples

An example of a data-integrity mechanism is the parent-and-child relationship of related records. If a parent record owns one or more related child records all of the referential integrity processes are handled by the database itself, which automatically ensures the accuracy and integrity of the data so that no child record can exist without a parent (also called being orphaned) and that no parent loses their child records. It also ensures that no parent record can be deleted while the parent record owns any child records. All of this is handled at the database level and does not require coding integrity checks into each applications.

File systems

Some file systems provide internal data and metadata check summing, what is used for detecting silent data corruption and improving data integrity. If a corruption is detected that way and internal RAID mechanisms provided by those file systems are also used, such file systems can additionally reconstruct corrupted data in a transparent way. This approach allows improved data integrity protection covering the entire data paths, which is usually known as end-to-end data protection.

Data storage

Data Integrity Field (DIF) was an approach to protect data integrity in computer data storage from data corruption. It was proposed in 2003 by the T10 subcommittee of the International Committee for Information Technology Standards. Packet-based storage transport protocols have CRC protection on command and data payloads. Interconnect buses have parity protection. Memory systems have parity detection/correction schemes. I/O protocol controllers at the transport/interconnect boundaries have internal data path protection. Data availability in storage systems is frequently measured simply in terms of the reliability of the hardware components and the effects of redundant hardware. But the reliability of the software, its ability to detect errors and its ability to correctly report or apply corrective actions to a failure have a significant bearing on the overall storage system availability. The data exchange usually takes place between the host CPU and storage disk. There may be a storage data controller in between these two. The controller could be RAID controller or simple storage switches. DIF included extending the disk sector from its traditional 512 bytes, to 520 bytes, by adding eight additional protection bytes.^[1] This extended sector is defined for Small Computer System Interface (SCSI) devices, which is in turn used in many enterprise storage technologies, such.

Data corruption

Data corruption refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data. Computer, transmission and storage systems use a number of measures to provide end-to-end data integrity, or lack of errors.

In general, when data corruption occurs a file containing that data will produce unexpected results when accessed by the system or the related application. Results could range from a minor loss of data to a system crash. The image to the right is a corrupted image file in which most of the information has been lost.

Some programs can give a suggestion to repair the file automatically (after the error) and some programs cannot repair it. It depends on the level of corruption, and the built-in functionality of the application to handle the error. There are various causes of the corruption.

Apart from data in databases, standards exist to address the integrity of data on storage devices.

• Overview

There are two types of data corruption associated with computer systems: undetected and detected. Undetected data corruption, also known as *silent data corruption*, results in the most dangerous errors as there is no indication that the data is incorrect. Detected data corruption may be permanent with the loss of data, or may be temporary when some part of the system is able to detect and correct the error; there is no data corruption in the latter case.

Hardware and software failure are the two main causes for data loss. Background radiation, head crashes, and aging or wear of the storage device fall into the former category, while software failure typically occurs due to bugs in the code. Cosmic rays cause most soft errors in DRAM.

• Silent

Some errors go unnoticed, without being detected by the disk firmware or the host operating system; these errors are known as *silent data corruption*.

There are many error sources beyond the disk storage subsystem itself. For instance, cables might be slightly loose, the power supply might be unreliable, external vibrations such as a loud sound, the network might introduce undetected corruption, cosmic radiation and many other causes of soft memory errors, etc. In 39,000 storage systems that were analysed, firmware bugs accounted for 5–10% of storage failures. All in all, the error rates as observed by a CERN study on silent corruption are far higher than one in every 10^{16} bits. Web shop Amazon.com has acknowledged similar high data corruption rates in their systems.

users are capable of transferring 10^{16} bits in a reasonably short time, thus easily reaching the data corruption thresholds.

Silent data corruption may result in cascading failures, in which the system may run for a period of time with undetected initial error causing increasingly more problems until it is ultimately detected.^[12] For example, a failure affecting file system metadata can result in multiple files being partially damaged or made completely inaccessible as the file system is used in its corrupted state.

• Countermeasures

When data corruption behaves as a Poisson process, where each bit of data has an independently low probability of being changed, data corruption can generally be detected by the use of checksums, and can often be corrected by the use of error correcting codes. If an uncorrectable data corruption is detected, procedures such as automatic retransmission or restoration from backups can be applied. Certain levels of RAID disk arrays have the ability to store and evaluate parity bits for data across a set of hard disks and can reconstruct corrupted data upon the failure of a single or multiple disks, depending on the level of RAID implemented. Some CPU architectures employ various transparent checks to detect and mitigate data corruption in CPU caches, CPU buffers and instruction pipelines.

Data scrubbing is another method to reduce the likelihood of data corruption, as disk errors are caught and recovered from before multiple errors accumulate and overwhelm the number of parity bits. Instead of parity being checked on each read, the parity is checked during a regular scan of the disk, often done as a low priority background process. Note that the "data scrubbing" operation activates a parity check. If a user simply runs a normal program that reads data from the disk, then the parity would not be checked unless parity-check-on-read was both supported and enabled on the disk subsystems.

I Principle

ALCOA

1. *Attributable*

Attributable, The identity of the person creating a record should be documented. For paper records this is normally done by the individual signing and dating the record with their signature.

As the record you may be signing may be a legal document, you should clearly understand the implication of your signature.

A signature should be individual to a specific individual and the practice of signing someone else's name or initials is fraud and is taken very seriously.

2. *Legible*

A record that cannot be read or understood has no value and might as well not exist. All records should be composed so they conform to grammatical convention which should be consistent throughout.

It is best to avoid buzzwords, cliques and slang as these are prone to change with time and are often not understood outside a particular locality.

It is always good practice to have any record reviewed by a second person as this can often highlight any ambiguities.

3. *Contemporaneous*

All records must be made at the time an activity takes place. Delaying writing up, for example until the end of the day, will inevitably affect the accuracy of that record as details can be forgotten or miss-remembered.

4. *Original*

All records must be original; information must be recorded directly onto the document. This avoids the potential of introducing errors in transcribing information between documents.

If information from an instrument is printed out, by the instrument, that printout is the original record and should be signed, dated and attached to the record.

5. *Accurate*

The record must reflect what actually happened. Any changes should be made without obscuring or obliterating the original information, the use of whiteout or correction fluid is prohibited. Any changes made to a record should be signed by the person making the change and dated to show when it was made and a written explanation should also be provided. Remember, the record may be needed after you have left the company and cannot be contacted for clarification.^[20]

II. Principle

1. **Principle 1:** An adequate data control system including independent checks and balances must exist within and between operating units.
2. **Principle 2:** All employees engaged in financial management activities are responsible for ensuring that adequate data controls are being employed. If they are not, all employees must take an active role in developing and implementing appropriate corrective actions.
3. **Principle 3:** Each unit must ensure that recorded assets match actual existing assets. A mechanism must be in place to spot discrepancies and to ensure that corrective actions are taken.
4. **Principle 4:** Each unit must ensure that all financial transactions are recorded correctly. Correct transactions must:
 1. reflect the actual values involved,

2. contain sufficient detail for proper identification and classification,
3. be posted on a timely basis in the proper accounting period,
4. be stored securely,
5. be readily retrievable for inquiry or reporting, and
6. be safeguarded against improper alteration.

5. **Principle 5:** All systems that affect or are used to report financial data must be secure, reliable, responsive and accessible. These systems must be designed, documented, and maintained according to accepted development and implementation standards. They should be built upon sound data models and employ technology that allows data to be shared appropriately.

6. **Principle 6:** All financial systems should meet the users' needs. In addition, all interfaces affecting any financial system must contain controls to ensure the data is synchronized and reconciled.

7. **Principle 7:** All technical networks, including electronic mail, through which departmental users access University financial data must be reliable, stable and secure.

III. Responsibilities

A system of data integrity includes

A) Allowing no one individual complete control over all key processing functions for any financial transactions. Such functions include:

1. recording transactions into the Financial System directly or through an interfacing system,
2. authorizing transactions through preapproval or post audit review,
3. receiving or disbursing funds,
4. reconciling financial system transactions and
5. recording corrections or adjustments.

If insufficient personnel within the unit requires that one person perform all of these functions, the unit must assign a second person to review the work for accuracy, timeliness and honesty.

B) Ensuring that all employees who prepare financial transactions provide adequate descriptions, explanations, and back-up documentation sufficient to support post-authorization review and any internal or external audit.

C) Keeping "office of record" documents physically secure and readily retrievable. These documents must be retained for the periods specified in the University Records Disposition Schedules Manual.

D) Ensuring that staff reconcile transactions appearing on the general ledger at the end of each accounting period.

1. All transactions must be verified for:
 - a. amount,

- b. account classification (FAU),
- c. description, and
- d. proper accounting period.

1. All reconciliations must be performed in a timely manner.

A. Using exception reporting, variance analysis and other mechanisms to monitor, review and reconcile financial activity to ensure that:

1. Employees are adequately trained in preparing and processing financial transactions,
2. Transactions and balances that exceed control thresholds or counter policies, regulations or laws are questioned and thoroughly analyzed, with corrections or adjustments fully documented and processed in a timely manner,

3. Locally generated reports do not distort or misrepresent the source data used to prepare them. In particular,

a. one must be able to reconcile reports back to the original data, as it appears in the Financial System, and

b. any adjustments made in preparing a local report must be documented and recorded immediately, where appropriate in the Financial System All unit assets are properly described and accounted for in the Financial System or other "official books of record" and

Actual physical assets are compared to recorded assets in the Financial System and discrepancies are resolved in a timely manner.

A. Encouraging all employees to report any break down or compromise in the unit's data integrity without fear of reprisal.

For further information, contact Internal Audit

A reliable financial computing environment includes the following components:

A. A long-term administrative computing plan that follows a thorough assessment of all major business processing and data needs. The plan defines the technical infrastructure and each of the system projects required to meet the unit's needs for the next three years. The plan should be updated annually.

B. Experienced and well-trained technical professionals to meet the unit's computing needs, including as a *minimum*, a *Computing Support Coordinator*.

The Agency Organisations

MHRA -Regulates medicines and medical devices, ensuring that they work and are acceptably safe; focusing on the core activities of product licensing, inspection and enforcement and pharmacovigilance.

Designated UK Competent Authority for Blood safety and quality.

- **Clinical Practice Research Data link (CPRD)** -Gives access to an unparalleled resource for conducting observational research and improving the efficiency of interventional research, across all areas of health, medicines and devices.

- **National Institute for Biological Standards and Control (NIBSC)** -World leaders in assuring the quality of biological medicines through product testing, developing standards and reference materials and carrying out applied research.

- **Corporate divisions** –Communications, human resources, operations and finance, information management, policy.

General Regulatory Guidance for Data Integrity

- USFDA –Draft Guidance 2016 and 21 CFR part 11
- EU GMP - Chapter 4 Annex 11
- MHRA- Draft Guidance 2016
- ICH Q 7 - Computerised Systems Section 5.4
- WHO TRS 937, Annex 4, Appendix 5
- GAMP 5 Introduction to Regulations.^[13]

Data Integrity Guidance

- UK MHRA-GMP Data Integrity Definitions and Guidance for Industry-March 2015
- USFDA –Data Integrity and Compliance with CGMP.
- WHO –Good data and Record Management Practices
- PIC/S & TGA –Basic Data Integrity Expectations.^[18]

FDA Draft Guidance on Data Integrity

the FDA issued draft guidance for industry on data integrity and compliance with cGMP. 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?^[20]

MHRA GMP Data Integrity Guidance for Industry

Designing systems to assure data quality and integrity. Systems should be designed in a way that encourages compliance with the principles of data integrity.

Examples include

- Access to clocks for recording timed events
- Accessibility of batch records at locations where activities take place so that ad hoc data recording and later transcription to official records is not necessary
- Control over blank paper templates for data recording
- User access rights which prevent (or audit trail) data amendments
- Automated data capture or printers attached to equipment such as balances
- Proximity of printers to relevant activities
- Access to sampling points (e.g. for water systems)
- Access to raw data for staff performing data checking activities.^[3]

The use of scribes to record activity on behalf of another operator should be considered 'exceptional' and only take place where:

- The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators.
- To accommodate cultural or staff literacy / language limitations, for instance where an activity is performed by an operator, but witnessed and recorded by a Supervisor or Officer.

In both situations, the supervisory recording must be contemporaneous with the task being performed, and must identify both the person performing the observed task and the person completing the record. The person performing the observed task should countersign the record wherever possible, although it is accepted that this countersigning step will be retrospective. The process for supervisory (scribe) documentation completion should be described in an approved procedure, which should also specify the

Data Integrity Regulations

21 CFR Part 11 –August 2003

EU Annex 11 –June 2011

21 CFR Part 11

Electronic Records(ER)

"Any combination of text, graphics, data, audio, pictorial, or other information representation in digital

form that is created, modified, maintained, archived, retrieved, or Distributed by a computer system.”

Electronic Signatures (ES)

“A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signatures.”

21 CFR Part 11 introductions and history

• 21 CFR PART 11 establishes the criteria by which the U.S.

Food and Drug Administration (FDA) considers electronic records, electronic signatures and hand written signatures executed to electronic records to be Trustworthy, Reliable, and generally equivalent to paper records and hand written signatures executed on paper. activities to which the process applies.^[19]

General Regulatory Expectation for Data Integrity Computerized Systems

- Password control and Prevent access to unauthorized users.
- Desktop Controls: Date and time locking/Access to the windows explorer/Disable USB, CD and floppy drive/Restrict access to
- Application Soft wares: Define privileges/assessment and

Qualification/Audit

Trail, activation, backup, review, recording/protection of data from cyber and environmental/implement the back up and restoration procedure.

- Any calculations used must be verified
- Data generated in an analysis must be backed up
- All standards and reference solutions are prepared correctly With suitable records.
- Data and reportable value must be checked by a second individual to ensure accuracy, completeness and conformance with SOPs.

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.^[6]

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 SOP 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.^[5]

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.

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 then tire 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.^[7]

The various types of documents followed in pharma industry are as follows:

Specifications: the document which lists out the active and inactive starting materials, packaging materials, intermediate, bulk and finished pharmaceutical products in terms of their physical, chemical and biological characteristics. The QC personnel will compare their test results to these specifications for the evaluation of the quality of the product.

Procedures and Test methods: these are written and approved documents which provide detailed instructions

for performing testing, operating the instrument, other production related tasks etc.

Records and reports: records are the documents completed by the manufacturing departments and includes protocols, log books etc. Report provides the data regarding conduct of manufacturing procedures along with results, conclusions and recommendations.

Master documents: These include master formula records, site master file, calibrations master plans, batch processing and packaging records etc. this ensures the uniformity from batch to batch.

Lists: It contains the full catalog for example list of equipment etc.

Documents or records should not be handwritten wherever necessary.^[10]

Causes of data integrity issues

- Data review limited to printed records- No review of e-source Data.
- Shared identity and passwords.
- Effective training to new entrants.
- Adherence to procedures and Standard Operating Procedures (SOPS).
- Following regulations and cGMP requirements.
- Lack of quality culture.
- No verification during self-inspections.
- Incomplete or altered data
- Backdating/Fabricating/Discarding
- Testing into compliance.
- Changing integration parameters of chromatographic data to obtain passing results.
- Turning off Audit trails capabilities
- Password sharing
- Inadequate controls for access privileges
- One batch Test results were used to release other batches.^[14]

General Data Integrity Issues

- Back dating of Documents.
- Fabricating the record.
- Deleting data.
- Overwriting.
- Torn Records.
- Testing to Compliance.
- Misusing of Administrative Privileges.
- Altering Integration Parameters without justification.
- Performing Sample trial injection.
- Invalidating OOS without justification or investigation.^[15]

General Data Integrity Issues (But Not limited to)

- Falsification in the context of GMP Compliance: Any will ful misstatement, misinterpretation, manipulation, rewriting, Hiding of quality related documents, materials, activities etc.
- Concealing a known problem

- Improperly altering operating conditions.
- Use of improper calibrations and verifications
- Fabricating, Falsifying or misrepresenting data, including creating data for a test that was not performed.
- Omitting or deleting data for tests that were performed where the results were not favorable.
- Turning off or disabling electronic instrument audit trails.^[16]

Common data integrity issues

Some of the common issues that repeatedly come up in FDA warning letters are:

- Common passwords- Where analysts share passwords, it is not possible to identify who creates or changes records, thus the A in ALCOA is not clear.
- User privileges- The system configuration for the software does not adequately define or segregate user levels and users have access to inappropriate software privileges such as modification of methods and integration.
- Computer system control- Laboratories have failed to implement adequate controls over data, and unauthorized access to modify, delete, or not save electronic files is not prevented; the file, therefore, may not be original, accurate, or complete.
- Processing methods- Integration parameters are not controlled and there is no procedure to define integration. Regulators are concerned over re-integration of chromatograms.
- Incomplete data- The record is not complete in this case. The definition of complete data is open to interpretation—see references 13 and 14 for a detailed analysis of FDA 483 observations on complete data (21 CFR 211.194 and sub parts).
- Audit trails- In this case, the laboratory has turned off the audit-trail functionality within the system. It is, therefore, not clear who has modified a file or why.^[10]

Requirements to have compliance to data Integrity

- Management Support.
- Robust Quality System.
- Effective Training.^[17]

Laboratory Data Integrity in FDA Warning Letters 2012

1. Test Results / (Raw) Data

The test results reported are not considered valid.

HPLC test results were not consistently calculated.

There is no assurance that the assay values reported for these samples are accurate and reliable.

Specifically, indicate if the discarded data pertained to lots shipped to the US and your justification for invalidating the data.

Lack of quality oversight and poor CGMP documentation practices at your facility, specifically in

the area of the disposition and handling of critical analytical data.

In your response, include your remediation plan to ensure that raw data is retained as required, along with the written procedure describing the retention and disposition policy for all laboratory control records.

Printed copies of HPLC test results from your firm's systems do not contain all of the analytical metadata (for example: instrument conditions, integration parameters) that is considered part of the raw data.

Please state the additional preventative and systemic actions you will implement to assure integrity of all CGMP records.

Your firm has not established appropriate controls designed to assure that laboratory records include all data secured in the course of each test, including graphs, charts and spectra from laboratory instrumentation.

The FDA investigator's review of the HPLC ... raw data verified the existence of three (3) HPLC chromatograms generated from batch However, only two (2) injection areas were used in the calculations.

An analytical worksheet for ... , lot ... , dated January 21, 2011, with no approval signature, was found in a trash container in the office used by QC personnel. This analytical worksheet shows calculations of content uniformity for active ingredient of ... %.

Any written report of results (including a certificate of analysis) to your customer should include a statement that the data was generated by an invalidated method(s) and should not be used for establishment of expiration dates, commercial batch release, or other CGMP decisions.

(Your firm has) failed to maintain complete records of all testing and standardization of laboratory reference standards and standard solutions.

Given the lack of maintenance records, it was unclear how long the filter light had been on or if the filters had been replaced since installation.

Data is deleted to make space for the most recent test results. You also informed our investigators that printed copies of HPLC test results are treated as raw data.

2. Written (Control) Procedures

Your firm failed to establish and follow written procedures to evaluate, at least annually, the quality standards of each drug product to determine the need for

changes in drug product specifications or manufacturing or control procedures.

Your quality control laboratory has not followed written procedures for testing and laboratory controls.

The inspection revealed that your firm has not established written procedures to control and account for electronically generated worksheets used by analysts to record analytical test results. Analysts in your QC laboratory print an uncontrolled number of worksheets from computers throughout the QC laboratory without supervision.

3. Computerised Systems

Your firm did not put in place requirements for appropriate usernames and passwords to allow appropriate control over data collected by your firm's computerized systems including UV, IR, HPLC and GC instruments.

Also describe your firm's policy for retaining HPLC raw electronic data associated with pending applications.

We also note that your SOP does not have provisions for any audit trail reviews to ensure that deletions and/or modifications do not occur.

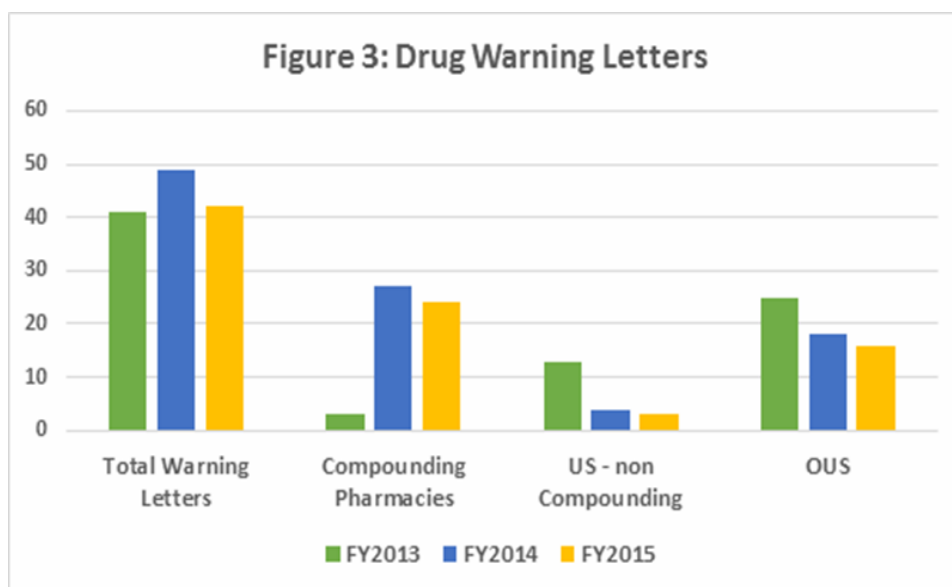
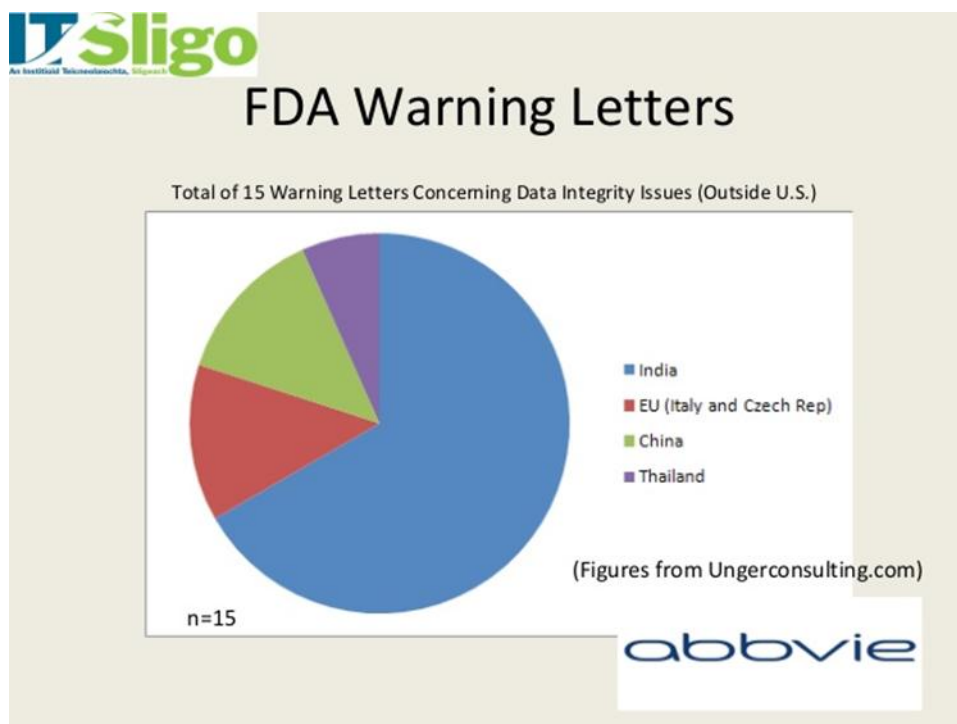
You have not implemented security control of laboratory electronic data.

There is no system in place to ensure that all electronic raw data from the laboratory is backed up and/or retained.

During the inspection, you informed our investigators that electronic raw data would not exist for most HPLC assays over two years old because data is not backed up and storage space is limited.

The chemist only reported two injection areas to produce the result (according to review of electronic data from testing of assay).

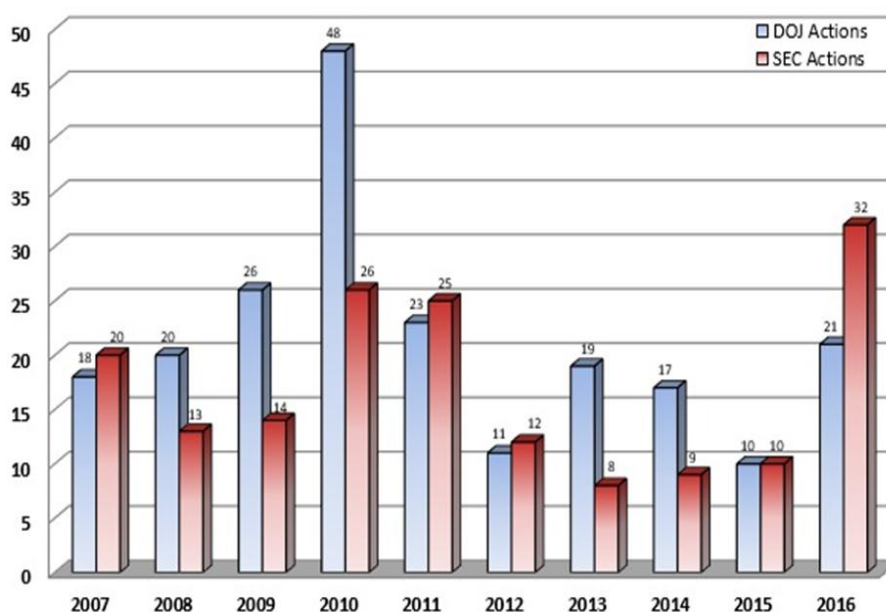
Without proper documentation, you have no assurance of the integrity of the data or the functionality of the software used to determine test results. Your firm had no system in place to ensure appropriate backup of electronic raw data and no standard procedure for naming and saving data for retrieval at a later date.^[12]



FDA Enforcement Statistics Summary Fiscal Year 2016

Enforcement Type	FY 16 Summary Numbers
Seizures	4
Injunctions	17
Warning letters	14590
Recall Events	2847
Recalled products	8305
Drug Product Debarments	1
Food Importation Debarments	0

Number of FCPA Enforcement Actions Per Year



Recommendations for remediating and preventing issues

Based on this structured approach for characterizing and optimizing quality systems, there are five leading solutions for remediating and preventing data integrity problems:

1. Investigating and remediating data integrity issues through CAPA and other evolving quality systems.
2. Creating a culture of quality.
3. Developing visible, engaged leadership with commitment to continuous improvement.
4. Recruitment and retention strategies that support sound GMP and Good Documentation Practices (GDP).
5. Practical balanced performance management.

Specific findings must be managed; however, if systemic, the root cause generally requires a shift in culture. Data Integrity problems must be investigated and remediated effectively through CAPA and other quality systems. Specific actions will be tailored based on findings, and may include:

- **Greater accountability**, such as clear zero tolerance practices that people must be trained on as soon as they join the organization and greater focus on recruitment and retention.

- **Procedural changes** with increased training and development (e.g. enhancing Part 11 controls, investigations, internal/external audit programs, trending, segregation of duties, test run accountability and vendor/contractor management and agreements).

- **IT enhancements**, such as: configuration aligned with intended use, systems integration to minimize manual data transfer, addition of audit trails, single user access controls, and support for system back-ups.

- **Focused process mapping** and failure modes and effects analysis (FMEA) around problem areas such as GDP.

- **Ensuring that source data is ALCOA** – Attributable, Legible, Contemporaneous, Original and Accurate.

- **Risk based oversight may be needed** in cases with high regulatory risk. Earning and maintaining a “right-to-win” mentality is a central element of a culture of quality. Cultural transformation plays a critical role in ascending the compliance maturity curve, with structured assessments including periodic culture surveys, helping to tailor continuous improvements.^[8]

Data Integrity – How to minimize the Risks

There are ways to minimize threats to data integrity. These include

- Segregation of Duties (SOD)
- Configuration of systems
- Backing up data regularly
- Controlling access to data via security mechanisms
- Designing user interfaces that prevent the input of invalid data
- Using error detection and correction software when transmitting data
- Audit trail Review.
- Data Integrity Policy.
- Technology & Procedural Control.
- Risk Assessment – Data Flow.
- Instrument/System/Computer Qualification & Validation Training.
- Auditor Qualification.
- Review Mechanism.

- Escalation & Governance (Transparency & Encouragement)
- Data Integrity Internal Audit Systems.
 - Risk Based
 - Independent Auditor
 - Fresh Eye
 - Surprise Audits
 - Appropriate Frequency
 - Review - Difficult Methods/Systems, OOS, Deviations, Complaints
 - Focus – Raw Data V/s Reports V/S Sample Log
 - Standalone Systems.
 - Lab Documentation Practices.
 - Review of Training Programme.^[18]

Segregation of duties Roles and Responsibilities allowing a conflict of interest that would allow alteration of data. For example, the QC Lab Manager acting as system administrator for Empower would violate segregation of duties.^[4]

-The PDA “Points to Consider Elements of a Code of Conduct for data Integrity” provides a good basis for a Data Integrity Policy with its scope covering: Good Manufacturing Practice (GMP), Good Clinical Practice (GCP), Good Pharma covigilance Practice (GVP), Good Laboratory Practice (GLP), Good Distribution Practices (GDP), Good Tissue Practice (GTP).^[9]

mitigate Data Integrity risks

- Review of Audit Trails
- Data Integrity Audits

audit trail

For purposes of this guidance, audit trail means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. An audit trail is a chronology of the “who, what, when and why” of a record. For example, the audit trail for a high performance liquid chromatography (HPLC) run could include the user name, date/time of the run, the integration parameters used and details of a reprocessing, if any, including change justification for the reprocessing. Electronic audit trails include those that track creation, modification, or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file). CGMP-compliant record-keeping practices prevent data from being lost or obscured (see §§ 211.160(a), 211.194 and 212.110(b)). Electronic record-keeping systems, which include audit trails, can fulfill these CGMP requirements.

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^[5]

Reviewing Audit Trails Comprehensive Review

Purpose

- Multiple processing of data to “pass”
- Altering metadata to make results pass
- Hiding or altering data on reports sent to QA
- Uncovering persistent suspicious behaviour around security of data
- Deletion of data
- Altering system policies /configuration / settings without change control procedures
- To uncover possible cases of fraudulent behaviour.

Audit Trail – Challenges

- Entries in the audit trail have to be understandable
- The old and new value for a change must be recorded along with who made the change
- A reason for changing data may be required
- Entries must be date and time stamped

- The format of this must be unambiguous and many also require the time zone

- Audit trails need to be associated with the activities supported and it must be possible to search the entries for specific events

• Audit trails must be secure from change

• Audit trails have to be retained for the record retention period

- The minimum period is at least (5 years = regulatory requirement)

Data integrity can no longer be assured by documentation, testing and security alone.

Auditing Data Integrity

1. Audit how the business use systems and data against applicable regulations, standards, and internal controls

2. Audit how systems are configured to meet business requirements

* Check of the Data Integrity should be part of the internal audit program

*Frequency will depend on the data risk for the safety of the patient and the quality of the product

CONCLUSION

Data integrity is everyone's responsibility. As an increase in problem of data integrity in giant pharmaceutical companies, there is a need of proper and effective documentation and record maintenance in pharmaceutical companies.

REFERENACE

1. boritz, J "IS Practitioners views on core concept of information integrity". international journal of accounting information systems. Elsevier archived from the original on 5 October 2011.
2. data integrity and Compliance With CGMP Guidance for industry.
3. wolfgang Schumacher , F. Hoffmann-La Roche, " Ensuring data integrity in the pharmaceuticals Industry – mitigation of risks "April 2016.
4. wolfgang Schumacher , F. Hoffmann-La Roche, " Ensuring data integrity in the pharmaceuticals Industry – mitigation of risks "April 2016.
5. 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>.
6. World Health Organization. (2016). Guidance on good data and record management practices.
7. Review of Good Data Integrity Principles.
8. Marie R. McDonald, Vice President, Quintiles IMS Consulting Services, Glen Potvin, Senior Director, Quintiles IMS, " Good Manufacturing Practice data integrity problems on the rise: *Risks, causes and practical solutions*".
9. Centre of biopharmaceuticals Excellence Data Integrity In the Global Pharmaceutical Industry.
10. Syed S Abbas, the author is the director of Institute of good manufacturing practices India (IGMPI),"documentations and records maintenance: A need for good manufacturing practices (GMP) Compliance in pharma & healthcare industry."
11. Paul smith, "Data integrity in Analytical laboratory".
12. Dr. Günter Brendelberger, CONCEPT HEIDELBERG, "Laboratory Data Integrity in FDA Warning Letters."
13. 13,14,15,16,17,18,19) Mr BHIMAVARAPU KOTI REDDY," Data integrity and compliance".
20. World Health Organization. (2016). Guidance on good data and record management practices.