QUALITY CONTROL • ALCOA + & TRAINING

DATA INTEGRITY IN QC

ALCOA+ | Inspection observations | Data review

01

DATA INTEGRITY IN QC

ALCOA+ — core principles

- A — Attributable: Authentication, Unique ID, Access permission
  Every activity or record must be traceable to the person who performed it (Who did it ?).
  System must verify the identity of the person accessing it (Is this person really who they claim to be ?)
  Every user must have an individual identification account (Does each person have their own account ?)
  Each user must be given access rights according to their job (What is this person allowed to do ?).
- L — Legible: Human readable, Usable format
- C — Contemporaneous: Recorded at the time of the event, audit trail
  (Audit trail is a secure computer generated, time stamped record that allows you to trace the creation, modification, or deletion of electronic data and other relevant activities)
- O — Original: Audit trail, record linking
  (Is it the original record or a verified true copy ?)
- A — Accurate: Reliable, calibrated
  (Record the actual rest results correctly, Use calibrated instruments, Verify calculations before recording results, Don't falsify or manipulate data, Ensure that recorded data matches the original source data)

02

INSPECTION OBSERVATIONS

Most common citation 1

- Firm failed to document production and process control functions at the time of performance.
- Operator recorded the amount of material dispensed before it was dispensed.
- Employees admitted they do not record activities at the time of performance.
- QA employee signed as reviewing and releasing a batch when he did neither.

05

INSPECTION OBSERVATIONS

Most common citation 2

- Firm blended out-of-specification batches with passing batches to meet specification.
- Failing results were often kept in separate folders and the failing data was not considered when making release decisions.

06

INSPECTION OBSERVATIONS

The most common citation 3

- Firm did not document laboratory activities at the time of performance.
- Pre-dating or backdating laboratory records Occurred for assay, loss on drying, sample weighing, and stability testing

.

07

INSPECTION OBSERVATIONS

Most common citation 4

- Firm failed to maintain complete information relating to the production and control of each batch.
- Records for 23 batches did not contain batch numbers, manufacturing dates, expiration or retest dates.
- Approximately 75 ripped batch production records (BPRs) were found in the garbage (some with failing results).

08

INSPECTION OBSERVATIONS

Most common citation 5 - original records

- Ten bags of torn or partially destroyed original records including CAPAs, preventative maintenance forms, and calibration records were found.
- Raw data was written on scratch paper and sometimes differed from the data in the BPR.
- Correction fluid was used on production records.

09

INSPECTION OBSERVATIONS

Most common citation 6

- Firm failed to thoroughly investigate any unexplained discrepancy or failure of a batch or any of its components to meet specifications, whether or not the batch has already been distributed.
- 4 batches of failing API were used in fifteen finished dosage batches.
- Failing assays were repeated until passing results were obtained.
- Environmental monitoring results were recorded as zero but actually had growth.

10

INSPECTION OBSERVATIONS

Most common citation 7 - testing practices

- "Unofficial" visual exam conducted for sterile injectables to remove vials with visible contamination so that the batch would pass the official visual exam (occurred at 2 firms).
- Used three different analytical methods until obtaining passing results.

11

INSPECTION OBSERVATIONS

Most common citation 8

- Firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records.
- Audit trails were disabled.
- A shared username and password was used by many analysts.
- Users were able to manipulate, delete, or overwrite electronic raw data.
- Firm's laboratory practice is to print chromatograms and delete electronic raw data files.

12

INSPECTION OBSERVATIONS

Most common citation 9 - complete laboratory data

- Firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards.
- "Trial" sample injection data was not kept as part of the data for a batch.
- Sample weights, sample preparation and sample dilutions were not retained.
- Deleted data detected in audit trails; overwriting data; ripped up data found in the garbage.

13

INSPECTION OBSERVATIONS

Most common citation 10 - microbiological data

- Not reporting microbiological counts.
- Hundreds of environmental monitoring samples were not collected.
- Some microbiological sample plates/tubes were missing from the incubator.
- No microbiological testing was conducted; however, microbiological test results were reported on the certificate of analysis (COA).

14

INSPECTION OBSERVATIONS

Most common citation 11 - certificates of analysis

- Data on the COA sent with the batches was different than the COA the firm retained on file.
- COA retest date was changed to an expiration date and listed as eleven months later.
- No raw data in support of results reported on COA.
- Samples with no identification were discarded during the inspection.

15

INSPECTION OBSERVATIONS

Most common citation 12 - HPLC and validation

- Firm deleted all electronic raw data supporting HPLC release testing.
- Standards were injected and used as sample results.
- Duplicate logbooks were kept.
- Complete raw data to support test method validation was not retained.
- Integration parameters for HPLC analysis were not retained.

16

PRACTICAL ACTIONS

How can you be part of the solution

- Look for gaps in how you control your records.
- Ensure employees have appropriate user privileges.
- Audit your data in a risk-based manner.
- Verify the authenticity of your contractors' data.

34

DATA INTEGRITY

What is mean by Integrity ?



1 **Principles:** Basic rules or standards that guide our actions and decisions. Employees must follow established rules when creating recording reviewing and approving data.

2 **Ethics:** Employees must behave honestly and professionally when handling laboratory data.

3 **Truth:** All recorded information must represent what actually happened during testing or manufacturing.

4 **Culture:** Management and employees must create a working environment where everyone follows data integrity requirements (The shared values, attitudes and behaviors of people in an organization)

5 **Sincerity:** Being genuine, honest and serious about your responsibilities.

6 **Code:** A set of written rules or standards that people are expected to follow (Employees must know what they must and must not do.

7 **Virtue:** A good personal quality or character trait. (Honest, responsible and discipline)

8 **Business:** An organization's activities to provide goods or services and earn revenue (The company must not conceal the problem simply to protect its sales or reputation)

9 **Reliability:** The ability to be trusted because something is accurate, consistent and dependable.

What is Integrity ?

Presentation Overview

- Objective of Data Integrity
- What is Data Integrity?
- Regulatory Requirement
- Data Integrity Principles
- ALCOA, + Principles
- Basic Data Integrity Expectations
- Data Integrity examples and WL
- Implementation
- Conclusions

Integrity: Direct meaning

Cambridge Dictionary:

Integrity noun [U] (HONESTY) ... the quality of being honest and having strong moral principles that you refuse to change

Quality & Integrity

"Quality Means Doing it Right When Nobody is Looking"



Integrity :
The Quality of being honest and having strong moral principles

Integrity : Can we say "BEING HONEST, EVEN WHEN NOBODY IS WATCHING"

Objective of Data Integrity

to ensure **patient safety** and **Quality**

- ....*the protection of the patient* by managing the risk to ***quality*** is considered as importance.
- *Ultimately Pharmaceutical quality is to* ***Assure every dose is safe and effective, free of contamination and defects.***



Regulators view



Data Integrity breach Break the trust between Industry and Regulatory Agencies .

Time period between the inspections, ***we trust you to do the right thing when the regulatory agency are not watching***.

If they **find compliance gaps**, ***regaining trust can be costly, and time consuming Task.***

Karen Takahashi
Senior Policy Adviser to USFDA

Data Integrity - purpose

- Assures the **Quality, Safety And Efficacy** of the dru g
- **DOCUMENTED RECORD** available to represent the Quality of the product after sold
- **Reliability of the data** is important
- Questioning Data Integrity = Loss of Trust
- **"Guilty until Proven Innocent"** to FDA
- Submitting false data to the FDA is a criminal violation



Manufacturing medicines for life-saving cannot afford to be negligent .

FDA have a "ZERO TOLERANCE" policy for data integrity

Bad practices



What are Poor or Bad practices ?

What is misconduct ?

What is Data falsification or fabrication?

Poor/Bad practices and Falsification

Innocent Ignorance	Carelessness/ Negligence	Intentional/ Malicious
Act is unintentional; Non-Compliance is	Act may or may not be intentional;	Act is intentional; Non-compliance is

Data Integrity

Are all misconducts are DI??

What are called Data Integrity breach ?

- Falsification / fabrication
- Dishonest / malicious
- Hiding
- Bad practice: historical practice, Shortcuts, etc

Data Integrity

Know the difference between Poor/Bad practices and Falsification

- Human errors data entered by mistake
- Ignorance (not aware of regulatory requirements or poor training)
- Errors during transmission from one computer to another
- Changes due to software bugs or malware of which the user is unaware
- Use of non-validated software applications/Spreadsheets
- Discarding source documents after accurate transcription;
- Hardware malfunctions
- Wilfully falsification of data or fraudulent data (with the intent to deceive)
- Selection of good or passing results (exclusion of poor or failing results)
- Unauthorised changes of post acquisition data - overwriting, change the name / data

FDA findings Related ~~Data~~ integrity

- Backdating/Postdating/missing /mismating Signatures
- Data manipulation/ data falsification,
- Copying existing data as new data
- Not saving the actual electronic or deleting electronic data after Printing- Chromatograms
- Disposing the original hard copies
- Not reporting of failures and deviations
- Releasing the failing product
- Hiding/obscuring /withholding critical information etc
- Mismatch between reported data and actual data

Is Data Integrity specific to country or region?



"Data Integrity Issue is across the Globe".

"It is not an India-centric or Asia centric problem".

What are the consequences of DI?

- The cost of remediation, investigation, CAPA to meet regulatory compliance will be huge when compared to prevention of DI.
  - It will destroy the image of the company
  - loose the credibility from customers,
  - demoralize the employees,
  - reduces time to gain the market
  - Affects the future plan of the company.....

Spending Rupees for prevention is better than spending in millions for remediation

Does any management wanted to have DI in their Organization?

Is top management aware all the problems?

How it is happening?

Why it is not identified and corrected?

Where is DI starts .....

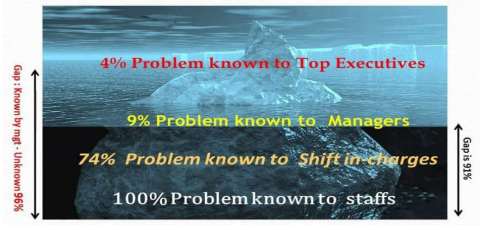
Where is DI starts & continues.. ?

- Organization culture
  - Employee awareness,
    - Taught by seniors
      - Motivation of wrong doing
        - Lack of Quality System
          - Lack of Infrastructure
            - Inadequate process / technology
              - Wrong understanding
                - Bad practices.....

How organization is missing to know or Possibility of ignorant

...Which may lead to DI

Iceberg of Ignorance



Data Integrity as per USFDA

Data integrity is critical to regulatory compliance, and the fundamental reason for 21 CFR Part 11.

DATA

- A - Attributable
- L – Legible
- C – Contemporaneous
- O – Original
- A - Accurate
- \+ Complete
- \+ Consistent
- \+ Enduring
- \+ Available



ALCOA principle

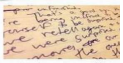
ALCOA is an acronym representing the following data integrity elements:

- Attributable – Who performed and when?
- Legible – Can it be read? Permanent Record
- Contemporaneous – Recorded at the time the activity was performed
- Original – Original record or certified true copy
- Accurate – Error free

Contemporaneous

- ⓘ Data entered in the record at the time of activities performed
- X Second person /witness **(eg weight)** enter the data by observer at the actual time; but second person only signing at end of the shift.
- X Electronic version of the excel output saved on personal drive and printed in a later time.
- X Time clock is not available/ accessible where the activity is performed. Eg. maintenance activity at near by /away
- X Unavailability of form, raw data sheet and log books right place.
- X Recording data in white paper /scrap papers / post it and entered the data in actual record later
- X Non compliance with Good documentation practices (back date /forward date).

Legible



- ✓ Hand writing should be readable by others. If Chemists hand writing is not readable like prescription, it will be assumption.
- ✓ Any correction shall be done as per Good Documentation Practices
- ✓ Data can not be obscured with a data annotation tool.
- ✓ Data printouts shall be readable. No smudged letters / fade ink cartridge / store the printed in thermal paper
- X Write over's - usage of correction fluids / Eraser or pencil .
- X Correct number of significant digits is not shown on the printout (Machine or Excel printout).

Attributable : Examples to DI

- ➢ Common User ID and password or sharing
- ➢ Disable of audit trail : Not able to identify the person who did the activities or changed.
- ➢ Admin user ID is as "Admin" and who is access? Not able to indentify.
- ➢ Analyst doesn't log out of PC in HPLC. Subsequent analysis is performed by second analyst under same login.
- ➢ Design of forms/ record: BPR does not have space for recording observation or additional information / signature.
- ➢ Two persons are performing the activity and one person signing.

Original

- X Modify / deleting the original data.
- X Operator writes down data onto scratch paper and then transcribes it onto the batch record.
- X Results written on to a new worksheet because original worksheet got smudged/ torn. Old sheet discarded.
- X Supporting data /raw data is discarded
- X Data printout is retained as raw data , original electronic record which contains meaningful metadata is discarded.

Accurate

- X Operator records a passing value for IPC result, even though they never performed the test, as they know this attribute never fails.
- X Actual result is failing , so data is discarded; the system adjusted to get passing results to avoid an OOS.
- X Flow meter readings are recorded with the "typical" value, rather than the (start and end) actual value.
- X Data is recorded on paper, however during transcription the numbers are accidentally reversed.
- X Data from passing run is re-named, and used for a different sample to ensure a result within specification.

+ Complete

- X Deleting selective data (deviation/OOS) and retaining desired data.
- X Worksheets/ notebooks not reconciled or controlled.
- X Data printout without instrument ID, analyst name, method name, or date, or time .... analysis.
- X Three technicians work on a complex calibration, but only one person's name is on the record.
- X Data printout is retained as raw data, original meaningful metadata is discarded.

+ Consistent

- X Batch record steps are filled inconstantly- based on the operators time.
- X Recorded info may found ambiguity in the process or data, which may be due to inadequate design of worksheet / format. Eg parallel activity / sequential activity...
- X System flashes the results and the results disappears before operator can record the data. Eg rpm of reactor/cfg
- X System allows you to preview data prior to naming or saving the record.

+ Enduring

- X Thermal paper is used for equipment printouts, but copies are not made available.
- X New software upgraded for the system, but existing data could not be retrieved due to old version of software
- X Poor quality of printed report/ BPRs
- X Record the data in temporary manner and forget . Eg QC chemists writes in butter papers, post-it notes, etc.,
- X Not storing the data from the system / not taking backup

+ Available

- OOS results are hideout in separate folder and frequently deleted.
- Files are not backed up, and data is deleted from the system periodically .
- Records are not archived until its complete retention period.
- Validated spreadsheet is not backed-up.

Data Integrity :

Computer Systems

Data Up & Recovery

- Procedure for data back up
- Electronic records should be available until retention period
  - Back-up, archival and recovery
  - Primary & secondary back up
  - Preferably auto back up
  - Disaster recovery / Business continuity planning
- Evidence for Back-up and recovery.
- Validation and verification at defined frequency

Computer System – Access Control

- Prevent unauthorized access to systems and altering any data
- Do not use common id & password
- Do not share user ID & password
- Password Polices
- Job /role specific access
- Lowest access level possible to perform the job to highest level to control overall by IT or QA
- Do not use common system administrator account
- Must ensure that any changes to records be made only by authorized personnel
- System administrator should be different from those with substantive responsibility

Data integrity issues

- Disabling audit trails in electronic data capture systems
- No /Inappropriate Audit Trail
- Conducting unofficial analysis /Re-running samples / Test until release
- Inadequate Access Authorization/ Privileges
- Discarding Deleting of data/ omitting negative data (like OOS or eliminating outliers)
- Not reporting failing results /stability failures
- Fabricating training data
- Having unofficial batch sheets and analytical reports

The above are not related to training or understanding technical or Quality Concept, but

mainly related to honesty and ethical issues.

Typical content in WL

- Firm did not identify, report, or investigate the out-of-specification (OOS) results.
- Firm did not retain any raw data related to sample weights and sample solution preparations for the HPLC assays and repeated the analysis next day using a new set of sample solutions, and reported the retest results in COA
- Firm deleted /disregarded OOS data without investigations, and selectively reported only passing results.
  - During inspection, QC Chemist admitted that, under the direction of a senior colleague, he had recorded false data in the logbooks **for reserve samples**

Typical content in WL

- The documentation is first done on loose sheets of paper and recorded in batch record.
- "QC analyst label sample "trial" injections as standard rather than by the actual sample batch numbers"
- Company deleted multiple HPLC data files acquired
- The FDA found an operator performing in process weight checks memorizing two " weights" , going to the next room where the batch records are kept and documenting the same
- Creating acceptable test results without performing the test
- Access control is not implemented in GC, FTIR and HPLC to prevent unauthorized access and control
- Backdating stability test results to meet the required commitments

Typical content in WL

Firm repeatedly delayed, denied, limited an inspection or refused to permit the FDA inspection:

- Torn raw data records in the waste area ,asked to QA Officer to show these for inspector's review. QA Officer removed 20 paper records
- Inspector asked three times if there were any more records and the QA Officer responded to each question, "no, this is all of the records".
- Inspector then re-visited the waste area and found that the raw data records had been removed and placed in a different holding bag.
- These records included raw data testing worksheets, MB report BPR calibration records, and stability protocol records.
- **All area will be accessed or copying of records for the FDA inspection.**

Recent WL on DI

1. **Failure to have laboratory control records that include complete data derived from all laboratory tests conducted to ensure your API complies with established specifications and standards.**

- Our investigator found that your firm was falsifying laboratory data. For example, the number of colony-forming units (CFU) found on **(b)(4)** plates for **(b)(4)** water point-of-use tests differed substantially from the number recorded on your **(b)(4)** water report. For multiple points of use, your analyst reported far fewer CFU than observed on the plate by our investigator. In addition, while you reported absence of growth on a selective media plate used to detect objectionable microorganisms, our investigator observed growth on this plate.

Observations in vendor audit

- pH written in BMR 7.00 by checking using pH paper
- Temperature recording as 78. 0°C in analog indicator
- Record of 20.03kg in the balance has 0.05kg least count
- Tare weight of poly bags 0.250kg in all the bags
- Vacuum 750mm throughout the operation including breaking for sampling
- Testing time is prior to the sampling time
- >20 reading in the same order /same alignment (as like home work)
- Record the weight /yield without fractional value 20.000 /210.000
- Mismatch of activity between records eg maintenance work, power trip, BPR Vs maintenance records

Recent WL on DI

- *Your firm failed to establish an adequate quality control unit with the responsibility and authority to approve or reject all components, drug product containers, closures, in-process materials, packaging materials, labeling, and drug products (21 CFR 211.22(a)).*
- Your quality unit (QU) lacks appropriate responsibility and control over your drug manufacturing operations.
- During the inspection, our investigator observed discarded CGMP **documents and evidence of uncontrolled shredding of documents**. For example, multiple bags of uncontrolled CGMP documents with color coding indicating they were from drug production, quality, and laboratory operations were awaiting shredding. **Our investigator also found a blue binder containing CGMP records, including batch records for U.S. drug products, discarded with other records in a 55-gallon drum in your scrap yard.** CGMP documents in the binder were dated as recently as January 21, 2019: seven days before our inspection. Your QU did not review or check these documents prior to disposal.

Opportunity Vs Motivation Vs Control



Control Failures
- Unclear or inadequate procedures
- Lack of control over forms and / or samples
- Controls not forcing accountability
- Disjointed electronic systems
- Too many transcription steps

Motivators
- Pressure to succeed
- Lack of training /
- Multiple reviews (next reviewer will find the mistake)
- Operational inefficiencies
- Frequent failure / unstable process
- processes not well understood

Motivation and Control

- If the motivation is high enough, no level of control will be sufficient
- Too many controls, different level may be drivers for higher motivation for untoward data manipulation
  - Too many review, initiator may believe that reviewer will find mistake
  - Many review cycles may slow down work and increase work pressure
- If processes is well understood , issues will be less including DI
  - Understand risks in the processes
  - Do not live with issue
  - Understand and correct them

Implementation

Strategy:	Develop strategy, identify and get support from management
Culture	Build into organizational culture & to change the mindset and behavior
Training	Provide appropriate training. Involve teams and bring initiatives
Detection	Identify thro strong Internal audit, IPQA , audit trail . Identify regulatory expectations
Prevention	Incorporate / build into the system, Risk Assessment / internal audit on DI

Tips for Data Integrity - Implementation

- Establish a "Data Integrity policy" .
- Describe the DI and consequences of DI breach /falsification of data
- Training on the DI policy or procedure .
- Establish a GDP so that even the most innocent recording issues cannot be perceived as fraudulent
- Design systems to prevent DI
  - Keep the BPRs / Log books / at work place to assess and record
  - Control over templates/ formats/ blank papers
  - Setting proper access to users/ audit trail
  - Connect recorder / printouts /
  - Access to Clock for recording time

Data Integrity - Implementation

Prevention – better than cure!!!



- QMS modernisation
- Computer System Validation
- Data review policy
- Quality Risk Management Processes
- Control of documents/ records
- Strengthen internal Audit
- Identifying risk factors
- Technical/QA Training/Education
- Promoting and supporting Quality Culture
- Effective CAPAs –Systemic Assessment all the area
- Quality Management Performance Review Meetings etc

Design the system to prevent DI

Systems should be designed to assure data integrity.
Examples not limited to ;

- Access to clocks for recording timed events
- Access to sampling points / displays/ measuring devices
- Access to raw data for staff for review
- Accessibility of batch records at locations where activities take place so that adhoc 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

Area to focus

People
- Technical/QA Training/Education Rate–All employees with direct impact on product/data
- Effectiveness of Training/Education
- Management Accountability for Cultural development; promoting and supporting quality

Places
- Investment spent in new and existing facilities, equipment, utilities

Performance
- Frequency of Quality Management Performance Review Meetings
- Level of proactive actions and assessing trends

Prevention
- Quality Risk Management Processes
- Internal Audit Programs
- Effective CAPAs –Systemic Assessment all the area

Data Integrity – What you have to do?

- Be Honest
- Record / Enter the date & time as per procedure
- Enter the data and sign or initial on the original records in a contemporaneous manner
- Data shall be accurate
- Never record pre-date or back date entries
- Keep inform superior in case deviation



Let us Question ourselves

- Are we compliant with the ALCOA Principles in our daily work?
- Do we meet the requirements of regulatory Guidelines?
- Where do we have problems or deviations regarding data integrity?
- Which employees have difficulties with implementation?
- Do we live by the principles of a comprehensive quality culture?
- Is quality a critical factor for the company's decision processes?

Ref documents

- PIC/S Guidance Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments - November 2018
- MHRA'GXP' Data Integrity Guidance and Definitions March 2018
- FDA : Data Integrity and Compliance With CGMP Guidance for Industry April 2016

No nightmare



THANK YOU

FOR YOUR ATTENTION

info@ishasgmp.com
ishasgmp@gmail.com
project@ishasgmp.com

Head Office:
Isha's GMP Consultancy Pvt Ltd,
Regency flat, Sri Hi-Tech construction,
5566, 1st cross street, CRR puram, LNT colony, Manapakkam, Chennai-600125

+91 8667589984
+91 9976491578

www.ishasgmp.com

