

DATA INTEGRITY: EXPECTATIONS & EXPERIENCE IN GLP

DR. L.U. SANGHANI
DIRECTOR – QUALITY ASSURANCE UNIT, JRF GLOBAL

SCOPE OF PRESENTATION

- **Data Integrity**
- **Expectations**
- **Common Pitfalls**
- **DI Contributing Factors**
- **DI Audit in GLP Quality System**
- **DI Audit- Audit Trail**
- **User Authentication Procedure**
- **Data Integrity - Self Audits**
- **DI: Chromatography Concerns**
- **Typical DI Audit Observations**
- **Data Integrity – Procedures / SOPs**

DATA INTEGRITY

- Data integrity is the degree to which data are complete, consistent, accurate, trustworthy, reliable and these characteristics of the data are maintained throughout the data life cycle.
- Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate(ALCOA).
- Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices.

EXPECTATIONS

- ❖ Adequately validated computerised systems
- ❖ Sufficient controls to prevent unauthorized access or changes to data.
- ❖ Implement a data integrity lifecycle concept
- ❖ Security, user access and role privileges (Admin)
- ❖ Activate audit trail and its backup
- ❖ Procedure and records for audit trail review
- ❖ Backup, archiving arrangements
- ❖ Disaster recovery plan
- ❖ Verification of restoration of raw data
- ❖ Qualification and change control

COMMON PITFALLS INCLUDE

- ❖ Perception of a lack of quality culture
- ❖ Design and configuration of systems are poor
- ❖ Data review limited to printed records - no review of e-source data
- ❖ System admin within Analyst/QC, can delete data
- ❖ DI is not only a QC lab issue
- ❖ DI awareness training/refresher absent
- ❖ DI verification not part of self inspections
- ❖ QA oversight of CS negligible
- ❖ Shared Identity/Passwords

DI CONTRIBUTING FACTORS

- ❖ Leadership and KPIs can drive wrong behaviours
- ❖ Inappropriate system design encourage bad practices
- ❖ Culture of fear, blame and punishment
- ❖ Poor attitude to problems- miss learning opportunities
- ❖ Poor training, staff lack DI awareness
- ❖ Don't care, won't get caught attitude
- ❖ Lack culture of quality, doing it right when nobody is watching
- ❖ Insufficiently controlled processes and Poor documentation practices
- ❖ Suboptimal quality oversight
- ❖ Wilful, intentional data falsification
- ❖ Old computerized systems

DI AUDIT EXPERIENCE-GLP

- ❖ Review of paper only systems, controls, loose sheets
- ❖ Review of networked systems at a PC
- ❖ Review of data on standalone equipment
- ❖ More audit time in the analytical lab and for manual records
- ❖ Traceability of raw data-test item receipt to use
- ❖ Review of raw data for ongoing studies
- ❖ Review of time specific activities and access control data

DI AUDIT IN GLP QUALITY SYSTEM

- ❖ What document systems used?
- ❖ GLP computerised inventory list?
- ❖ Review of the Procedures dependent on pre-set parameters
- ❖ Audit of Test Item and Reference Standards inventory
- ❖ Review of sensitive equipment calibration and maintenance
- ❖ Dose formulation preparation, dilution and sampling
- ❖ Work distribution to study personnel and technicians
- ❖ Corrections/modification of data-justification and authorization

DI AUDIT- SAMPLE HANDLING

- ❖ Test Item receipt log- date, time, name, quantity, use and disposal
- ❖ Sample container labels, verify physical sample
- ❖ Check the retained samples, periodic examination
- ❖ Check for QC samples without evaluation criteria
- ❖ Test time reflects time of sample collection etc.
- ❖ Re-sampling events

DI AUDIT- AUDIT TRAIL

- ❖ Is the audit trail activated? SOP?
- ❖ Record of reviews?
- ❖ Training of staff on audit trail review?
- ❖ Is predicate rules followed for changes?
 - ✓ preserve original data
 - ✓ corrected data
 - ✓ date of correction
 - ✓ name of person who corrected the data
 - ✓ justification comment for correction

USER AUTHENTICATION PROCEDURE

- ❖ Procedure to add, modify and delete users
- ❖ Employees leaving the company removed from system?
- ❖ Training requirements before access is granted.
- ❖ Clear roles and responsibilities of users
- ❖ Procedure for (re-)activating passwords, including identification process of the user requesting a new password and procedure for the communication of the password.
- ❖ Administrators should not have a conflict of interest.
- ❖ Periodic reviews performed?
- ❖ Do you have sufficient user licences for your systems

DATA INTEGRITY - SELF AUDITS

- ❖ Train auditors using industry & in-house examples
- ❖ Do unannounced audits, Quality walks etc.
- ❖ Focus on raw data handling & data review/verification procedure
- ❖ Verify signatures against a master signature list
- ❖ Look for unofficial or private records
- ❖ Check inventory system – Receipt against actual usage.
- ❖ Check test system source, receipt and use records
- ❖ Check adequate control of lab records – re-issues, discard of raw data
- ❖ Verify use & existence of equipment in laboratory
- ❖ Interview study personnel and technicians

DI: CHROMATOGRAPHY CONCERNS

- ❖ Deletion of data, Folders & individual data files
 - ✓ Software not properly monitored
 - ✓ Non-compliant software used
 - ✓ Analysts not properly trained
- ❖ Overwriting of data
- ❖ Altering integration parameters
- ❖ Performing sample trial/test/demo injections
- ❖ Administration and user privileges
- ❖ Lack of audit trail and data reviews

TYPICAL DI AUDIT OBSERVATIONS

- ❖ Trial injections.
- ❖ Results failing specifications are retested until acceptable results are obtained.
- ❖ Over-writing electronic raw data.
- ❖ OOS not investigated as required by SOP.
- ❖ Appropriate controls not established.
- ❖ Records are not completed contemporaneously
- ❖ Back-dating, Fabricating data.
- ❖ No saving electronic or hard copy data.
- ❖ Records completed for absent employees

FDA 483 OBSERVATIONS

- ❖ Overlap of time for different experimental stages
- ❖ Records filled prior to actual execution
- ❖ Copy & rename existing data as new data
- ❖ Mismatch between reported data and actual data
- ❖ No traceability of reported data to source documents

DATA INTEGRITY – PROCEDURES / SOPs

A set of SOPs to be in place to support Data Integrity and minimise risk within GLP facility:

- ❖ IT policies.
- ❖ System administration (CDS access, roles and privileges).
- ❖ Data management and storage.
- ❖ Data acquisition and processing.
- ❖ Data review and approval.
- ❖ Data archiving and back-up.
- ❖ Anti-fraud monitoring.

CONCLUSION

- ❖ Data integrity is not always easy to detect -educate
- ❖ Understand the strengths and weaknesses of the systems used to collect, store and process raw data
- ❖ Comply with the regulatory expectations
- ❖ Staff training awareness and refresher programs
- ❖ Establish an integrated self audit program
- ❖ Develop a strong quality culture
- ❖ Speak up for quality



THANKS

Indian Regional Forum

Presented by : Labhu Sanghani, Director - Global QA, Jai Research Foundation

