Data Integrity Audits: pitfalls, expectations & experiences

Mark Dickson
Senior Compliance Professional
Compliance & Inspection
Pharma Quality, Novartis

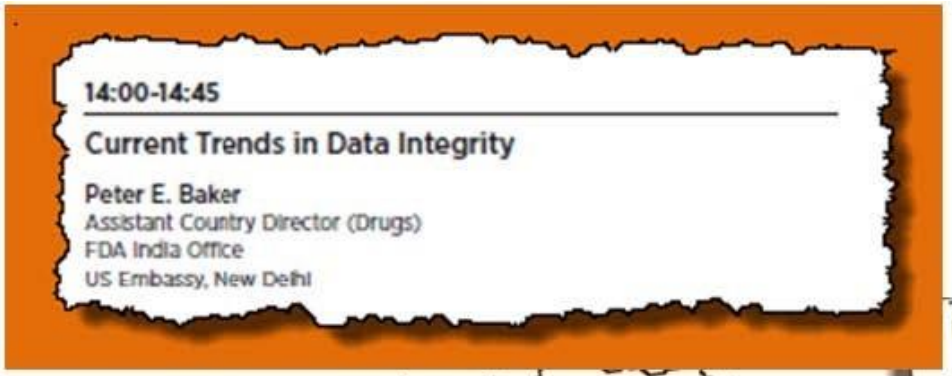
Disclaimer

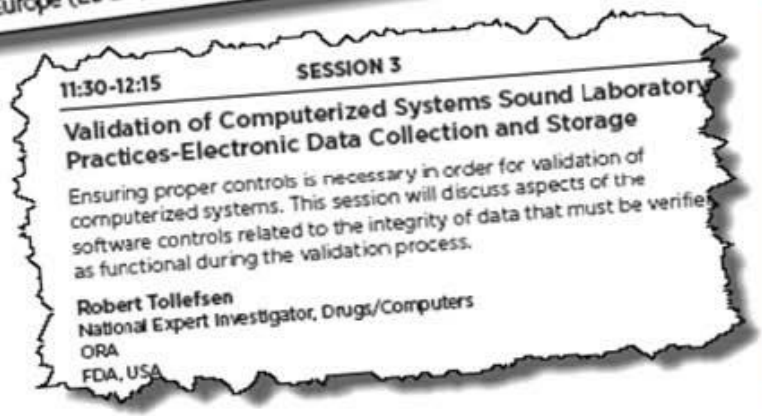
- *This presentation is based on publicly available information;*
- *These slides are intended for educational purposes only and for the personal use of the audience. These slides are not intended for wider distribution outside the intended purpose without presenter approval;*
- *The views and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of Novartis or any of its officers.*

Data integrity – reality in 2015

- Is it an old issue - good documentation practices?
- Do Health Authorities have new tools?
- Inspectors are trained & share learnings globally
- Unannounced & in depth inspections on the increase
- Inspector tolerance low; but high alert to DI problems
- Consequences can be severe
- Regaining trust is difficult – global systematic CAPA
- DI breaches are found worldwide
- DI found by FDA, MHRA,EDQM,WHO, ANSM, etc.

FDA,EDQM & industry workshops across India, Nov 2014





DI workshops in Beijing June 2015

- Monica Cahilly leading trainer and consultant
- FDA's Peter E. Baker, Assistant Country Director
- Gang Wang, FDA Assistant Country Director

Recent DI publications includes:

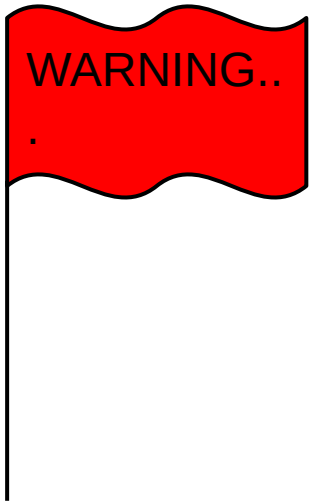
- MHRA GMP Data Integrity Definitions & Guidance for Industry, March 2015
- MHRA DI blogs: org behaviour, ALCOA principles
- FDA Warning Letters and Import Alerts
- EUDRA GMDP database noncompliance
- HC Feb 2015 stakeholders letter incl. DI notification
- HC Inspection tracker for GMP and DI observations
- Guidelines expected from FDA and WHO
- CFDA preparing GMP Annex: CSV

Expectations - computerised systems

- Adequately validated and have sufficient controls to prevent unauthorized access or changes to data.
- Who can delete data, change the clock etc.?
- 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, red flags 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 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 CMO's 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

DI contributing factors

- Insufficiently controlled processes
- Poor documentation practices
- Suboptimal quality oversight
- Professional ignorance
- Wilful, intentional data falsification
- Old computerized systems not complying with part 11 or Annex 11

DI Audit experiences

- DI overview absent in opening presentation
- The skill level of the auditor & auditee is variable
- More audit time in the QC lab, 1-5 days
- Traceability of raw data start to end common, **«---»**
- Review of raw data in the lab
  - Review of paper only systems, controls, loose sheets
  - Review of networked systems at a PC
  - Review of data on standalone equipment
- Takes time. Captures QMS elements by default
- MHRA requesting DI policy

DI audit -start with the walk through

- What document systems used?
- GMP computerised inventory list?
- What manufacturing systems dependent on pre-set parameters?
  - DCS, MES, IPC lab
  - Checkweighers, barcodes, PLC configured equipment
  - Sterilizers, filter integrity testers, BMS etc.
- Paper systems – batch record, logbook, forms
- How do they manage changes to these systems ?
- Use of Chinese/Hanko signature stamps

Sample handling

- Sample receipt log- date, time, name, qty, reconciled. Useful place to start.
- 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.
- Resampling events

Ask for the raw data

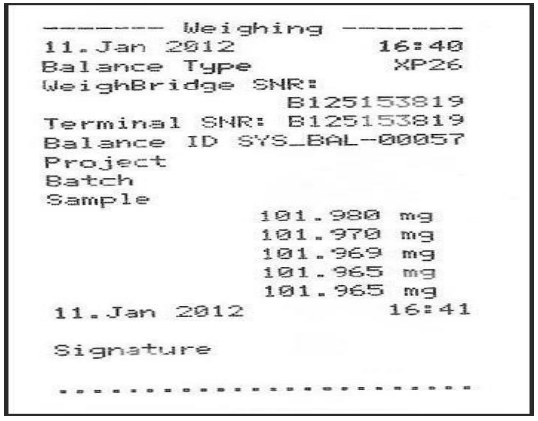
- Waste paper bins with raw data
- Shredder outside QC lab
- Data transfers to USB
- Lost/overwritten back ups
- Requested backups can't be restored
- Authorisation for restore, recovery, retrieval

Now think- audit trail off, QC Admin, deleted data!

Balances, FT-IR, UV, KF etc.

- Printouts same type and quality of paper/ink?
- Data recorded “too good to be true”, reference stds
- Change of date/time for winter/summer recorded
- Admin level, configuration, audit trail function
- Contemporaneous entries, discarded printouts?
- Where is the raw data saved?

Print the spectra (sample and reference) on one page for comparison purpose with the related parameters.



What to look for in audit trail

- Is the audit trail activated? SOP?
- Record of reviews?
- How to prevent or detect any deletion or modification of audit trail data? Training of staff?
- Filter of audit trail
- Is predicate rule principle followed for changes?
  - Preserve original data
  - corrected data
  - date of correction
  - name of person who corrected the data
  - justification comment for correction
- What if there is no audit trail function?
- “Can you prove data manipulation did not occur?”

Part 11 compliant systems?

Can a vendor guarantee compliant software for Part 11?

- It is not possible for any vendor to offer a turnkey 'Part 11 compliant system'. Any vendor who makes such a claim is incorrect. Part 11 requires both procedural controls (i.e. notification, training, SOPs, administration) and administrative controls to be put in place by the user in addition to the technical controls that the vendor can offer. At best, the vendor can offer an application containing the required technical elements of a compliant system.

User Authentication Procedure

- Procedure to add, modify and delete users
- Employees leaving the company removed from system?
- Training requirements before access is granted.
- Clear user roles and responsibilities 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?

EU Annex 11 vs 21CFR Part 11

- Differs from Part 11 in some definitions, audit trail requirements, application of risk management.
- Small difference in scope definition
- Annex 11 much more explicitly addresses risk
- 15 specific items not covered in Part 11:
  - 1 (Risk Management) -lifecycle approach;
  - 3 (Suppliers and Service Providers)-agreements ;
  - 4.1 (Validation Life Cycle);
  - 4.3 (Systems Inventory list and GMP Functionality);
  - 4.4 (User Requirements Specifications);

EU Annex 11 vs 21CFR Part 11

- 15 items not specifically covered in Part 11:
  - 4.5 (Quality Management System) of vendor/supplier;
  - 4.6 (Formal assessment for Customized Systems);
  - 4.7 (Evidence of Appropriate Test Methods & scenarios);
  - 7.2 (Back-ups);
  - 8.2 (Batch Release Records);
  - 12.2 (System Criticality controls);
  - 13 (Incident Management –reported & assessed);
  - 15 (Batch Release using e-signature);
  - 16 (Business Continuity); and
  - 17 (Archiving).

Perform Data Integrity self audits

- Embed DI verification in self inspection processes
- Train auditors in industry & in-house examples
- Do unannounced audits, Quality walks etc.
- Spend time in the lab or manufacturing, late shifts
- Focus on raw data handling & data review/verification
- Awareness of all GMP related staff – refresher GMP
- Consider external support to avoid bias

Global trends for new CMO use

- Person-In-Plant (PIP) for CMO's at early stage of project
- PIPs must be a cultural fit with the CMO, must have the credentials and the technical expertise, and must be trusted by the sponsor and the CMO.
- Avoid superficial audits of CMO's –risk unidentified subcontracting show and shadow factories
- Avoid a CMO site or sister site with a warning letter where possible due to the risk if same QMS
- How many other clients? CMO have any of their own products?
- Risk their own or client's products give negative inspection outcome?

Karen Takahashi, Snr Policy Advisor FDA-ISPE Oct 2014

- Detailed Data Integrity inspections

"The Mind-Numbing Way FDA Uncovers Data Integrity Laps", Gold Sheet, 30 January 2015.

- Start with the Lab when sniffing out Data Integrity

"The Gold Sheet, 19 Dec 2014"

FDA style DI audit

1. Verify the expected sequence of activities: dates, times, quantities, identifiers (such as batch, sample or equipment numbers) and signatures.
2. Constantly double check and cross reference
3. Verify signatures against a master signature list
4. Verify against time cards and employment history
5. Look for unofficial or private records
6. Check inventory system - material receiving records against actual usage. Verify point 1 above.

FDA style DI audit

7. Check source of materials received label, CoA, QMS
8. Verify times tested in lab for in-process, finished product, and stability testing with time in the batch record. Check logbooks vs raw data
9. Review batch record for inconsistencies
10. Review qty in shipping records against batch yield.
11. Check manufacturing capacity of the line
12. Check adequate control of lab and production records – re-issues, discard of raw data

FDA style DI audit

12. Verify use & existence of equipment in manufacturing, packaging and laboratory- check equipment logs, maintenance records, equipment purchase records, cleaning and calibration records.
13. Use equipment use logs to reconcile batches made
14. Interview staff not the managers

Now, the US FDA Investigators located in India and China are also (forensic) experts in Data Integrity !


WARNING
LETTERS
AND 483s

FDA's chromatography concerns

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

Typical DI observations

- Alteration
- Fabrication
- Misrepresentation
- Omission
  - Deliberate wilful deception - fraud;
  - Inadequate data or documentation retention practices;
  - Questionable, poor or incomplete documentation practice
  - Altering information on the certificate of analysis
- Is QA oversight lacking? Symptom of weak QMS?
- Why not found internally/previously?

FDA 483 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 for…."
- "….records are not completed contemporaneously"
- "… back-dating...."
- "... fabricating data..."
- ".... No saving electronic or hard copy data..."

FDA 483 observations

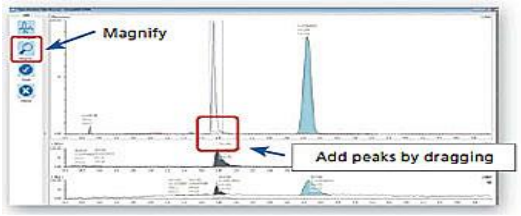
- Records completed for absent employees
- Overlap of time for different manufacturing stages
- Records filled prior to actual execution
- Copy & rename existing data as new data
- Mismatch between reported data and actual data
- No traceability of reported data to source documents

Possible consequences

- Risk to patients
- Drug shortages
- A scapegoat for the DI issues
- Regulatory filings affected
- Business reputation harmed
- Warning Letter and Import Alert (many markets)
- Consent Decree and fines
- Battle to regain trust of public, clients and Regulators
- Expect many other HA inspections & client audits
- $$$$ to remediate and hire 3rd party consultants

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
- Be patient centric




ANY
QUESTIONS
?


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
dank je
спасибо
dziękuję
obrigado
sukriya
kop khun krap
go raibh maith agat
mochchakkeram
arigatō
dakujem
grazie
terima kasih
merci
bedankt
감사합니다
мерси

- **In warning letters to firms, why has FDA objected to the practice of using actual samples to perform system suitability testing (sometimes also referred to as "trial," "test," or "prep" runs)?**FDA wants to discourage the practice of "testing into compliance." In some situations, the use of actual samples to perform system suitability testing can be a means of testing into compliance. (See the guidance for industry *Investigating Out-of-Specification Results.*http://www.fda.gov/downloads/Drugs/Guidances/ucm070287.pdf)
- According to USP, system suitability tests should include replicate injections of a standard preparation or other standard solutions to determine if requirements for precision are met (ref. USP General Chapter <621> *Chromatography*). System suitability tests, including the identity of the preparation to be injected and the rational for its selection, should be performed according to the firm's established written procedures and the approved application or applicable compendial monograph (§ 211.160).
- If an actual sample is to be used for system suitability, it should be a properly characterized secondary standard and written procedures should be established and followed (§ 211.160 and 211.165). All data should be included in the data set that is retained and subject to review unless there is documented scientific justification for its exclusion.