DATA INTEGRITY, GAP ANALYSIS AND AUDIT

Karen Ginsbury
PCI Pharmaceutical Consulting Israel
IVT DI and Val Week
Amsterdam, March 2017
DISCLAIMER

■ KAREN GINSBURY IS A CONSULTANT

■ Your company has a Quality System and Quality Unit

■ Karen will make you think about things once again, but you MAY NOT change anything from approved SOPs because “Karen said so”

■ Any changes must go through the change control / change management process and be discussed and agreed internally with your Quality Unit
Elements of a data governance plan

- Policy
- Educate
- Communicate
- Technology and IT
- Audit and CAPA
ALCOA+

- Accurate
- Legible
- Contemporaneous (real time)
- Original
- Attributable

- Accurate
- Complete
- Consistent
- Secure
What would you look at

■ Group 1 – Gap analysis

■ Group 2 – Internal audit

questions...
Your firm did not thoroughly investigate lot #1129BX014, when it failed to meet the established specification for both the single largest impurity and for total impurities amount.

- Specifically, the laboratory test results had a single impurity at RRT 0.8 minutes of 0.34 (specification limit NMT 0.3% and total impurity result of 1.05% (specification limit NMT 1.0%)

- Your firm subsequently invalidated these results although your investigation was unable to confirm a root cause of the failure

- Your firm selectively used passing results from a different analysis to approve the lot
The Guidances – Harmonization? 
TWO kinds: Culture / QS vs Q&A

<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Aug 2016</td>
<td>EMA: Good Manufacturing Guidance to Ensure the Integrity of Data</td>
<td>23 Q&amp;A</td>
</tr>
<tr>
<td>10 Aug 2016</td>
<td>PIC/s: Draft Guidance Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments</td>
<td>41 pages</td>
</tr>
<tr>
<td>July 2016</td>
<td>MHRA: GXP Data Integrity Draft Guidance</td>
<td>14 pages</td>
</tr>
<tr>
<td>April 2016</td>
<td>FDA: Draft Guidance: Data Integrity and Compliance with GMP Q&amp;A</td>
<td>13 pages</td>
</tr>
<tr>
<td>March 2015</td>
<td>MHRA: Data Integrity Definitions and Guidance for Industry</td>
<td>16 pages</td>
</tr>
</tbody>
</table>
How to reach compliance and present the plan to regulators with metrics

- What DI behavior would you like to change?
- What could you measure?
The purpose of metrics is to change behaviors / to stimulate action

- Password usage being unique always
- How many audit trails show “user #1” rather than a name
- How many manual integrations are performed (look at why and are you comfortable with the amount or do methods need revision)
Altering time and date stamps

routine inspections of computerized systems may reveal gaps in security controls that inadvertently allow personnel to access and potentially alter time/date stamps. These findings help raise awareness to management of need to allocate resources to improve computerized systems validation controls;

WHO guidance
reduce data integrity risks. For example, identifying and addressing technical difficulties of equipment used to perform multiple GxP operations may greatly improve the reliability of data for all of these operations; identifying security conflicts and allocating independent information technology (IT) personnel to perform system administration for computerized systems, including managing security, backup and archival, reduces potential conflicts of interest and may greatly streamline and improve data management efficiencies.

WHO guidance
QU evaluate configuration settings
data annotation tools...

In addition, key personnel, including managers, supervisors and quality unit personnel, should be trained in measures to prevent and detect data issues. This may require specific training in evaluating the configuration settings and reviewing electronic data and metadata, such as audit trails, for individual computerized systems used in the generation, processing and reporting of data. For example, the quality unit should learn how to evaluate configuration settings that may intentionally or unintentionally allow data to be overwritten or obscured through the use of hidden fields or data annotation tools; supervisors responsible for reviewing electronic data should learn which audit trails in the system track significant data changes and how these might be most efficiently accessed as part of their review.

WHO guidance
Rename, copy, delete local files on stand alone system?

WHO guidance

• If users of stand-alone computerized systems are provided with full administrator rights to the workstation operating systems on which the original electronic records are stored, this may inappropriately grant permissions to users to rename, copy, delete files stored on the local system and to change the time/date stamp. For this reason, validation of the stand-alone computerized system should ensure proper security restrictions to protect time/date settings and ensure data integrity in all computing environments, including the workstation operating system, the software application and any other applicable network environments.
What is an OOS, OOT, Unusual, Questionable, “Atypical” Result

- Is it defined?
2. Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established specifications and standards.

Our investigators observed systemic data manipulation across your facility. They documented unexplained deletions of laboratory test results. They discovered that you repeated tests until you obtained acceptable results and that you failed to investigate out-of-specification or otherwise undesirable test results. Your firm relied on these falsified and manipulated test results to support batch release and stability data. Your firm routinely re-tested high performance liquid chromatography (HPLC) samples and deleted previous chromatograms without justification. Your management acknowledged that employees in your quality control laboratory have access, authority, and the ability to delete and repeat HPLC injections when undesirable results were encountered prior to reporting final results.

Your response states repeated testing was due to quality control operators continuously injecting solvents until a stable baseline was achieved. The response also states the results of repeated tests were deleted to decrease the number of saved chromatograms on your hard drives. Any data created as part of a CGMP record must be evaluated by the quality unit as part of release criteria and maintained for CGMP purposes. In order to exclude data from the release criteria decision-making process, you must have valid, documented, scientific justification for its exclusion.

Reducing the number of records on your hard drives is not a sufficient justification for excluding data. Your response is inadequate because you have not shown how you will correct the data manipulation and falsification practices discussed above, nor have you demonstrated how you will ensure that all CGMP test results are retained and considered by your quality unit as a part of batch release.
You do NOT want to go there...
Investigators are out of patience

B. A current risk assessment of the potential effects of the observed failures on the quality of your drugs. Your assessment should include analyses of the risks to patients caused by the release of drugs affected by a lapse of data integrity, and risks posed by ongoing operations.

C. A management strategy for your firm that includes the details of your global corrective action and preventive action plan. Your strategy should include:

- A detailed corrective action plan that describes how you intend to ensure the reliability and completeness of all of the data you generate, including analytical data, manufacturing records, and all data submitted to FDA.

- A comprehensive description of the root causes of your data integrity lapses, including evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. Indicate whether individuals responsible for data integrity lapses remain able to influence CGMP-related or drug application data at your firm.

- Interim measures describing the actions you have taken or will take to protect patients and to ensure the quality of your drugs, such as notifying your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, drug application actions, and enhanced complaint monitoring.

- Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of your company’s data.

- A status report for any of the above activities already underway or completed.
GIGO: ALCOA+
nothing lost, changed or manipulated

Data → Information → Knowledge

Analyze

Apply
Performed by....
Defined in an SOP

- To perform the action
- 100% responsible for the action and all activities associated with its performance and documenting its performance (may be electronic documentation)
Verified by...
Defined in an SOP

- To verify that the action was performed according to the current, written approved instructions

- 100% responsible for verifying that the action was performed correctly including all activities associated with its performance and the documentation of these

- MUST BE PRESENT THROUGHOUT AND WITNESS, THE PERFORMANCE OF THE ACTION AND ITS DOCUMENTATION before signing as verifier
The reviewer or approver
Defined in an SOP

- Approves data and analysis of the data – IS NOT PRESENT when the work is performed
- Should be provided with sufficient raw data and analysis to enable a complete and accurate review
WHO Guide pages 16 – 20
take a look

- Risk based approach outlining the particular risks for each aspect of ALCOA+
c) A “File Note” dated February 10, 2014, signed by the QC Head, established that the printed data used for batch disposition decisions from the Metrohm Titrando Instrument MLG/QC/12/048 hard drive was not necessarily the complete data for a batch. Our inspection found that data on the instrument was selected for use and was not protected from change and deletion. Notably, the audit trail capability of this QC “commercial” laboratory instrument was not enabled, even after creation of the “File Note.”
Backdating

- Our investigators found backdated batch production records dated February 10 to February 25, 2014, signed by your Production Manager and Technical Director in the “Batch Manufacturing Record Reviewed by” section.

- The Technical Director stated that he was not in the facility on these dates and was “countersigning” for another person who allegedly performed these review activities. However, these records did not contain signatures (contemporaneous or otherwise) of the alternate reviewer who purportedly conducted the review.

- Furthermore, the Technical Director backdated his own signature to the date the quality unit (QU) reviewed and released your drug product. You released these batches before the Technical Director returned to the facility and backdated his signatures.
Failure to record activities at the time they are performed and destruction of original records

- Specifically, your employees completed batch production records entries days after operations had ended, released lots before the proper approvals, and failed to maintain original manufacturing data for critical steps in the batch production records. For example, Our investigators found that some of your operators used “rough notes” (unbound, uncontrolled loose paper) to capture critical manufacturing data and then destroyed these original records after transcription into the batch production records.

- For example, the (b)(4) chemist recorded original manufacturing data as rough notes and left these rough notes for the (b)(4) chemist to transcribe into the batch production records. The next morning, the chemist signed the batch production records and destroyed the original rough notes. We interviewed employees during the inspection who confirmed your firm’s practice of transcribing data to batch records and destroying original records.
Shared Passwords

- 6. Your firm failed to establish appropriate controls over computers and related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel (21 CFR 211.68(b)).

- You lacked audit trails or other sufficient controls to facilitate traceability of the individuals who access each of the programmable logic controller (PLC) levels or Man-Machine Interface (MMI) equipment. You had no way to verify that individuals have not changed, adjusted, or modified equipment operation parameters. Access to production equipment used in parenteral manufacturing and solid dosage forms used a password shared by four or five individuals to gain access to each individual piece of equipment and access level.

- During our inspection, your Executive Production and QA manager confirmed that the password was shared. During our inspection, firm officials also confirmed that you had not established or documented a control program to describe the roles and responsibilities of production equipment system administrators. There was also no record documenting the individuals who have access to the production equipment or the manner in which individual personnel access production equipment.
Data Integrity: Paper / hybrid / Electronic

- Data is precisely recorded. On retrieval, the data is the same as when originally recorded, complete, consistent, accurate, attributable throughout the lifecycle (archiving, retrieval).

- The accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. Data integrity is imposed on a system at its design stage through standard rules and procedures, and maintained through error checking and validation routines.

- Critical aspect in the design, implementation and usage of any system which stores, processes or retrieves data.
Data integrity issues:

- Deletion – raw data
- Change – raw data
- Incomplete – raw data
- Unofficial or trial testing
- AA spectro – over 400 analyses – only 38 data files
- Audit trails deleted
- SOPs don’t include instructions for retention of raw data
- Date of second signature – what does SOP say?
- Disabled audit trail function
- Unauthorized file folders e.g. for column wash data
Original record vs True copy

■ **Original record**: Data as the file or format in which it was originally generated, preserving the integrity (accuracy, completeness, content and meaning) of the record, e.g. original paper record of manual observation, or electronic raw data file from a computerised system.

■ **True Copy**: An exact copy of an original record, which may be retained in the same or different format in which it was originally generated, e.g. a paper copy of a paper record, an electronic scan of a paper record, or a paper record of electronically generated data.

MHRA, Data Integrity Definitions and Expectations and Guidance for Industry, January 2015
Original record vs True copy

- Raw data generated by electronic means may be retained in a paper or pdf format. The data retention process must be shown to include verified copies of all raw data, metadata, relevant audit trail and result files, software/system configuration settings specific to each analytical run*, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set. It would also require a documented means to verify that the printed records were an accurate representation. This approach is likely to be onerous in its administration to enable a GMP compliant record.

- * computerised system configuration settings should be defined, tested and ‘locked’ as part of computer system validation. Only those variable settings which relate to an analytical run would be considered as electronic raw data.

MHRA, Data Integrity Definitions and Expectations and Guidance for Industry, January 2015
Have you defined (in an SOP)...
Educated and communicated...
Verified understanding of...

- Data
- Raw Data
- Meta Data
- Derived Data
- Original Record
- Primary Record
- True Copy
- Certified Copy
Some risks

- Paper based: missing signatures, details
- Excel spreadsheets
- Stand alone software
- Log on / log off
- Printouts vs unintegrated data
Audit trail and controls at two levels:

- **System Life Cycle**
  - Planning and Specifications
  - Development
  - Verification and acceptance
  - Operation and Maintenance
  - Retirement

- **Data Life Cycle**
  - Data Creation
  - Data Processing
  - Data Review
  - Data Reporting
  - Data Retention
Minimize threats to DI by:

- 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

**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.
Data Governance

- **Senior management** is responsible for the implementation of systems and procedures to minimise the potential risk to data integrity, and for identifying the residual risk.

- Contract Givers should perform a similar review as part of their vendor assurance program.
Data Integrity Code of Conduct

- Annual signature of all employees that they are aware of it and followed it...what about MOST senior management / officers of the company???

- Culture?
a. The inspection documented that HPLC processing methods (including integration parameters) and re-integrations are executed without a pre-defined, scientifically valid procedure. Your analytical methods are not locked to ensure that the same integration parameters are used on each analysis. A QC operator interviewed during the inspection stated that integrations are performed and re-performed until the chromatographic peaks are “good”, but was unable to provide an explanation for the manner in which integration is performed. Moreover, your firm does not have a procedure for the saving of processing methods used for integration.

Your response did not include a description of the method by which chromatograph integrations are to be performed (e.g., what constitutes a chromatographic peak, how shoulder peaks are to be handled, etc.). In addition, your response did not include an audit of past chromatographic data to determine whether data used to support release and stability studies originated from appropriately integrated chromatograms.
the use of the Excel® spreadsheets in analytical calculations are neither controlled nor protected from modifications or deletion. The investigator noticed that the calculation for residual solvent uses an Excel spreadsheet that has not been qualified. We are concerned about the data generated by your QC laboratory from non-qualified and uncontrolled Excel spreadsheets.

In response to this letter, provide a retrospective evaluation of the analytical values reported where such Excel spreadsheets have been used.

CAN’T WE DO BETTER THAN EXCEL?
Computerized Spreadsheets

- Error in / incorrect formula
- Spreadsheet not protected or locked
- Data loss through inadvertent or intentional deletion, errors, computer issues
- Omitted, added or altered information
- Entry / transcription errors
In Conclusion: eyes open
P-D-C-A

- Know the basic concepts of Data Integrity
- Keep a close eye on OOS and EDUCATE everyone – up and down in the organization
- **Understand the use of audits**
  - *Formal: internal audit program*
  - *On-the-spot: sometimes and whenever a problem is suspected*
- Recognize that the opportunity with data integrity is to **DESIGN** controls **INTO** the computerized system
- People based systems are stumbling blocks and will ultimately fail
Links to guides

- EMA Data Integrity Guidance Q&A
  http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp#section17

- PIC/s Data Integrity Guidance
  https://www.picscheme.org/useruploads/documents/PI_041_1_Draft_2_Guidance_on_Data_Integrity_2.pdf

- MHRA: GxP Data Integrity Definitions and Guidance

- WHO: guidance on good data and record keeping

- FDA Data Integrity and Compliance with cGMP

- MHRA: GMP Data Integrity Definitions and Guidance
THANK YOU FOR PARTICIPATING

Questions ? ? ?

Find me
Karen@pcipharma.com