Data Integrity, Data Analysis and Monitoring
Contents:

• Regulatory requirements and guidelines
• ALCOA
• Data Integrity for computer, paper and hybrid systems
• Control of meta-data
• Data integrity strategies for compliance
• Checking for Data Integrity issues in practice
Directive 2003 / 94/ EC – Article 9

“The manufacturer shall establish and maintain a *documentation system* based upon specifications, manufacturing formulae and processing and packaging instructions, procedures and records covering the various manufacturing operations performed. Documents shall be *clear, free from error and kept up to date*. Pre-established procedures for general manufacturing operations and conditions shall be kept available, together with specific documents for the manufacture of each batch. That set of documents shall *enable the history of the manufacture of each batch ... to be traced*”
Directive 2003 / 94/ EC – Article 9

“For a medicinal product, the batch documentation shall be retained for at least one year after the expiry date of the batches to which it relates or at least five years after the (QP) certification ... whichever is the longer period”
Directive 2003 / 94/ EC – Article 9

“When electronic, photographic or other data processing systems are used instead of written documents, the manufacturer shall first validate the systems by showing that the data will be appropriately stored during the anticipated period of storage. Data stored by those systems shall be made readily available in legible form and shall be provided to the competent authorities at their request. The electronically stored data shall be protected, by methods such as duplication or back-up and transfer on to another storage system, against loss or damage of data, and audit trails shall be maintained.”
So what is Data Integrity?

• **Institute of Electrical and Electronics Engineers (IEEE)**
  – The degree to which a collection of data is complete, consistent, and accurate

• **Wikipedia**
  – Data integrity refers to maintaining and assuring the accuracy and consistency of data over the entire data life-cycle;
    • Ensure data is recorded exactly as intended
    • Upon later retrieval, ensure the data is the same as it was when it was originally recorded

• **MHRA (UK)**
  – The extent to which all data are complete, consistent and accurate throughout the data lifecycle

• **EU GMP**
  – ????
EU GMP: Chapters UPDATES

• Chapters in EU GMP
  1. Pharmaceutical Quality System  New 2013
  2. Personnel  New 2014
  3. Premises & equipment  New 2015
  4. Documentation  New 2011
  5. Production  New 2015
  6. Quality Control  New 2014
  7. Outsourced activities  New 2013
  9. Self inspection
EU GMP: Annexes

1. Sterile manufacturing
2. Biological products
3. Radiopharmaceuticals
4. Veterinary medicinal products
5. Immunological veterinary products
6. Medicinal gases
7. Herbal medicinal products
8. Sampling of starting materials
9. Liquids, creams & ointments
10. Metered dose inhalers

11. Computerised systems
12. Use of ionizing radiation
13. Invest. medicinal products
14. Products derived from blood
15. Qualification and validation
16. Certification by a QP
17. Parametric release
18. Withdrawn
19. Reference samples
EU GMP Annex 11: Computerised Systems

“Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.”
Records

• The records associated with the manufacture of a batch of product are just as important as the batch itself
  
  “if it isn’t written down it’s a rumour”

• Records must also be retained:
  – Safely and securely
  – 1 year after the expiry of the batch or 5 years after QP certification
  – Some will be kept for decades

• Records can be kept off-site
• Scanning
Archiving

• Archive records
  – “secure controls must be in place to ensure the integrity of the record throughout the retention period and validated where appropriate”

– Paper based records
  • Location that will protect them
  – Scan them into a computer system
    • Keeping the scanned copy is as secure
Data Integrity

• Big focus area for inspections
  – Applied to paper-based records as well as computer-based
  – Focus on ensuring that documents, record and data remain secure, accessible and unaltered until its expiry date
Where does it apply?

- Paper based systems
- Computer based systems
- Hybrid systems
- Don’t forget the meta data
What is Meta Data?

- Take a simple analysis trace

What Does it mean?

mV signal
What is Meta Data?

- Take a simple analysis trace

Operator: JDSMITH
Date: 14\textsuperscript{th} Oct 2015
Time: 09:15:45

Analyser ID: ph2
Sample Ref: B1002
Run No: 1

mV signal
Meta Data

• Data that describes the attributes of other data and provides context and meaning
• Examples:
  – Photos: Date and time when taken
  – Website: Hyperlinks and Tags
  – Graphs: Calculations and raw data
  – Records: Time of action and terminal used

• This data may be kept within the equipment
  – May need to download it from time to time
Types of Data Integrity fraud

• Unintentional issues
  – Are often the result of poorly designed processes and procedures, mistakes or lack of understanding

• Falsification
  – Are deliberate actions to deceive or mislead, including knowingly performing manipulation, omission or deletion
Examples

• Original HPLC data was purposefully destroyed to eliminate poor test results
• A cleaning logbook was lost
• A verification check was performed, but not recorded
• A worker corrected an error from a previous shift and did not clearly explain why the correction was made
• A worker signed a batch record with a colleague's signature
• A cleaning logbook was purposefully filled out and completed by a worker for cleaning that was never performed
• Key data is not backed up at the time it should have been and data is lost when the system crashes
ALCOA

• Attributable
  – Information is captured that identifies the source of the data

• Legible, traceable, permanent
  – Information is always readable

• Contemporaneously
  – Information is recorded at the time of data generation or event observation

• Original
  – Data should be used or presented as it was created the first time

• Accurate
  – Data can be verified as correct via repeatable calculation or algorithm or analysis
ALCOA +

• **Enduring**
  – Data are preserved and retrievable during the lifetime according to data type retention period

• **Complete**
  – All data are present

• **Available**
  – Data are conveniently accessible at any time

• **Consistent**
  – Data are compatible, free from variation and non-contradictory
Spreadsheets

• Are useful, simple and cheap to use
  – Often first created by an individual

• Potential problems:
  – No audit trail for:
    • When data was added
    • Change (overwriting of data)
    • Who altered any data
  – The accuracy of calculations
    • Plus altering them
  – The saving of data
    • Often on a general server with access to a whole group people
    • Can it be deleted?
  – Is data archived in the same way as paper-based records?
Spreadsheets

- **Cannot** be used to store GXP related information
  - Need to have a log of what you have and likely to need local approval by QA
- May be used – but only in limited cases
- Only if For Information Only
  - Not used to make decisions
  - Not the prime source of data
- Examples:
  - Log of deviations:
    - All actions recorded on paper-based forms
    - As long as not used to control when actions are taken
  - List of who can approve documents:
    - As long as a hard copy is printed and signed every time updated
# Reprocessing of events

<table>
<thead>
<tr>
<th>Sample name</th>
<th>Acquisition time</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volt.@100 Run 1</td>
<td>14:12:19</td>
<td>120215.003.rst</td>
</tr>
<tr>
<td>Volt.@100 Run 2</td>
<td>14:18:10</td>
<td>120215-004.rst</td>
</tr>
<tr>
<td>Volt.@100 Run 5</td>
<td>14:29:19</td>
<td>120215-007.rst</td>
</tr>
<tr>
<td>Volt.@100 Run 5</td>
<td>14:36:07</td>
<td>120215-007-20110809-173718.rst</td>
</tr>
<tr>
<td>Volt.@100 Run 6</td>
<td>14:39:58</td>
<td>120215-008.rst</td>
</tr>
<tr>
<td>Volt.@100 inj acc</td>
<td>14:43:58</td>
<td>120215-009.rst</td>
</tr>
</tbody>
</table>

Avoid “Testing into Compliance”
Primary Records and True Copies

- Batch records are never totally computerised
  - Paper forms and records used for certain activities
    - Line clearance sheets
    - Sterilisation charts
    - Printouts
  - These are *Primary Records*
    - You may keep these
    - You may scan or copy these
    - Both
  - Copy or scan is a *True Copy*
    - Only if an exact copy
  - Need to control what you do with these
    - Especially if not stored with the computer based record
Objective reporting

• Incorporate data integrity assessment and Reporting into self-inspection program
• Ensure a system is in place to record data integrity issues (e.g. CAPA)
  – Data integrity issues
    • Have had a problem
  – Data integrity weaknesses
    • An issue – but no evidence of a problem
Data Integrity strategy

• It starts at the top - Management Led
• Have a Policy on Data Integrity
• Know what systems you have
• Know where you have weaknesses
  – Plan to deal with these
• Have a category or system to flag issues up
• Train personnel
• Look for DI issues during Internal Audits
• Look for DI issues during External Audits
• Look for DI issues with any new projects
References

• EU GMP Directives and Guidelines:
  • https://ec.europa.eu/health/documents/eudralex/vol-4_en
  • Many regulatory authorities have produced Data Integrity Guidance documents:
    • FDA:
    • EMA:
    • PICS:
    • WHO:
    • MHRA (UK):
      • https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity