Data Integrity: Success by Design
Fat-finger, Falsification and Fraud

Presented by Trevor Schoerie
30 July 2015
## The 3 Fs of data integrity

### System design failures and design controls

<table>
<thead>
<tr>
<th><strong>Fat Finger</strong></th>
<th>An inadvertent mistake made by an operator during the course of their work that can be made either on <strong>paper</strong> or <strong>electronically</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Falsification</strong></td>
<td>An <strong>individual</strong> who deliberately writes or enters data or results with the intention to deceive.</td>
</tr>
<tr>
<td><strong>Fraud</strong></td>
<td>Collusion between <strong>two or more individuals</strong> who deliberately write or enter data or results with the intention to deceive.</td>
</tr>
</tbody>
</table>
World’s biggest medicines recall

The suspension follows audits of the company's manufacturing premises, which revealed widespread and serious deficiencies and failures in the company's manufacturing and quality control procedures, including the systematic and deliberate manipulation of quality control test data.

- 219 products immediately recalled
- 1650 export products cancelled

‘The Australian public should not forget how bad the manufacturing practices were at <the company> which prompted what may be the world's biggest medicines recall.’

Source
The Rogue Analyst

...... that he believed "a rogue analyst" had manipulated the test results, but "the defendant tried to downplay the seriousness of the matter".

Giving evidence, the former IT manager said:

“The MD said to me, 'What is happening with the computer? Is there any data still on it?' to which I replied, 'No, there is no data still on it, I've reformatted the computer,'" he told the court.

The MD then asked him whether a computer expert would be able to retrieve the data if they were to access the computer.

"Can you make it so the data is not retrievable by anyone?"

A horse called Jim

A German scientist, **Emil von Behring** discovered that diphtheria antitoxin present in certain animals' blood could be made into a serum and injected into humans. His development of serum therapy against the disease earned him the first Nobel Prize in Medicine in 1901.

Jim was retired from milk cart duties and enlisted into the production of serum. Unfortunately, Jim contracted tetanus between the 25th Aug. and 30th Sept. 1901 and was put down.

Tragically, blood drawn on the 30th Sept was **mislabelled**, the 24th Aug and released, it resulted in the death of 12 children.

This incident and a similar Smallpox vaccine incident lead to the passage of the Biologicals Controls of 1902, which established the Center Biologics Evaluation and Research and later the formation of the **FDA** in 1906.
MHRA – Data Integrity Definitions and Guidance for Industry & Blog

MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015

Introduction:
Data integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality. This document provides MHRA guidance on GMP data integrity expectations for the pharmaceutical industry. This guidance is intended to complement existing EU GMP legislation and the GMP standards published in Eudralex volume 4.

The data governance system should be integral to the pharmaceutical quality system described in GMP chapter 1. The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands. As such, manufacturers and analytical laboratories are not expected to implement an approach to data checking on a routine basis, but instead design and operate a system which provides an acceptable state of control based on the data integrity risk, and which is fully documented with supporting rationale.

“a new look at an old topic”

Blog
MHRA Inspectorate

Organisations: Medicines and Healthcare products Regulatory Agency

Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 1
David Churchward, 25 June 2015 — Compliance matters

Data integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality.

A robust data governance approach will ensure that data is complete, consistent and accurate, irrespective of the format in which data is generated or retained.
“There is a general misconception that data integrity failures only result from **acts of deliberate fraud**.

.... majority of issues relate to –
- bad practice,
- poor organisational behaviour and
- weak systems,
which create opportunities for data to be manipulated.

..... some basic behavioural, procedural and technical steps to significantly improve their systems.”

**MHRA – David Churchward**
Design Controls for Data

- Identify critical data
- Identify risks to different types of data
- Determine the level of confidence required
- Establish controls over the data lifecycle
- Generate proof (audit trails, checklists, summaries)
Identify critical data
CFR Part 11, Scope and Application

Three critical data criteria –

1. **Predicate rules** - e.g. approved, reviewed and verified - *in place of paper format*

2. **Submitted to the inspector** - *in addition to paper format, and that are relied on to perform regulated activities*

3. **Regulatory submission** - helped us determine critical steps or data.

**New FDA Draft Request for Quality Metrics – July ’15**
“in lieu of inspection”

APR data, cPk, lot acceptance rate, OOS rate, Complaint rate, CAPA effectiveness,
FDA Part 11 – Design controls

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- appropriate controls over systems documentation
- controls for open systems corresponding to controls for closed systems bulleted above (§ 145 11.30)
- requirements related to electronic signatures
CHAPTER 4

DOCUMENTATION

PRINCIPLE

Good documentation constitutes an essential part of the quality assurance system and is key to operating in compliance with GMP requirements. The various types of documents and media used should be fully defined in the manufacturer’s Quality Management System. Documentation may exist in a variety of forms, including paper-based, electronic or photographic media. The main objective of the system of documentation utilised must be to establish, control, monitor and record all activities which directly or indirectly impact on all aspects of the quality of medicinal products. The Quality Management System should include sufficient instructional detail to facilitate a common understanding of the requirements, in addition to providing for sufficient recording of the various processes and evaluation of any observations, so that ongoing application of the requirements may be demonstrated.

Suitable controls should be implemented to ensure the accuracy, integrity, availability and legibility of documents. Instruction documents should be free from errors and available in writing. The term ‘written’ means recorded, or documented on media from which data may be rendered in a human readable form.
Data integrity
PIC/S GMPs

Manual entry of critical data should be checked by a second person or managed as part of or a validated system

§4.20, 4.21, 6.17

c) Identification (initials) of the operator(s) who performed each significant step of the process and, where appropriate, the name of any person who checked these operations;

g) initials of the person who verified the testing and the calculations, where appropriate;

h) a clear statement of release or rejection (or other status decision) and the dated signature of the designated responsible person.
Definitions

approved, reviewed and verified

Verified  Witnessed  Checked
Approved  Authorised  Performed
Prepared
Technical Design Controls

1. System complexity / inherent data risk
2. User access, permissions
3. Transactional windows
4. Data structure and location
   - Dynamic vs static, hosted
   - File structure
   - Audit trails and metadata
5. Validation vs functional verification
1. System complexity
Data criticality and inherent integrity risk

No software

Simple software

Complex software

Printouts could represent original data

Printouts not representative
2. User Access

**System access**
Individual logins (always)

**User/group permissions**
Appropriate to an individual’s roles
No IT Department?
Independence of roles
PQS / QMS visibility

**Watch recently the departed**
(CC)
### 3. Transactional window

#### Data entry window, idle log off

<table>
<thead>
<tr>
<th>No</th>
<th>Added raw material?</th>
<th>Performed by</th>
<th>Checked by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure room and vessel is .....</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2  | Add 100 litres purified water  
Start the stirrer  
Add 0.3kg catalyst  
Add 2kg buffer  
Add 30kg lactose |              |            |
| 3  | Record the time: __________am/pm |              |            |

<table>
<thead>
<tr>
<th>No</th>
<th>Added raw material?</th>
<th>Performed by</th>
<th>Checked by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure room and vessel is .....</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Add 100 litres purified water</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Start the stirrer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Add 0.3kg catalyst</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Add 2kg buffer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Add 30kg lactose</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Record the time: __________am/pm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Data structure and location

- Dynamic, i.e. mirrored, DC, backed up?
- Business continuation planning?
- Data only or real process information
- Can be restored? With Audit trail and metadata?
- If hosted,
  - who else can see it?
  - Service Level Agreement?
  - Can company and other parties inspect?
Just data vs process information, i.e. importance of metadata?

<table>
<thead>
<tr>
<th>Date</th>
<th>TIC601</th>
<th>HIC601</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/07/2015</td>
<td>22.00</td>
<td>69.80</td>
</tr>
<tr>
<td>21/07/2015</td>
<td>23.00</td>
<td>68.30</td>
</tr>
<tr>
<td>22/07/2015</td>
<td>24.00</td>
<td>66.50</td>
</tr>
<tr>
<td>23/07/2015</td>
<td>25.00</td>
<td>62.10</td>
</tr>
<tr>
<td>24/07/2015</td>
<td>25.00</td>
<td>63.60</td>
</tr>
<tr>
<td>27/07/2015</td>
<td>25.00</td>
<td>80.90</td>
</tr>
<tr>
<td>28/07/2015</td>
<td>22.00</td>
<td>65.40</td>
</tr>
<tr>
<td>29/07/2015</td>
<td>21.00</td>
<td>53.80</td>
</tr>
<tr>
<td>30/07/2015</td>
<td>20.00</td>
<td>55.10</td>
</tr>
</tbody>
</table>
## Meta data vs just data?

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Temp. &lt; 25°C</th>
<th>% RH &lt;75%</th>
<th>Operator</th>
<th>Date/time</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/07/2015</td>
<td>Top rack</td>
<td>22.00</td>
<td>69.80</td>
<td>TS</td>
<td>20Jul15 06:07:28GMT</td>
</tr>
<tr>
<td>21/07/2015</td>
<td>Top rack</td>
<td>23.00</td>
<td>68.30</td>
<td>TS</td>
<td>21Jul15 06:09:26GMT</td>
</tr>
<tr>
<td>22/07/2015</td>
<td>Top rack</td>
<td>24.00</td>
<td>66.50</td>
<td>TS</td>
<td>22Jul15 06:14:15GMT</td>
</tr>
<tr>
<td>23/07/2015</td>
<td>Bottom rack</td>
<td>25.00</td>
<td>62.10</td>
<td>TS</td>
<td>23Jul15 06:06:78GMT</td>
</tr>
<tr>
<td>24/07/2015</td>
<td>Top rack</td>
<td>25.00</td>
<td>63.60</td>
<td>TS</td>
<td>24Jul15 07:01:25GMT</td>
</tr>
<tr>
<td>27/07/2015</td>
<td>Top rack</td>
<td>25.00</td>
<td>80.90</td>
<td>TS</td>
<td>27Jul15 06:11:55GMT</td>
</tr>
<tr>
<td>27/07/2015</td>
<td>Top rack</td>
<td>25.00</td>
<td>72.30</td>
<td>TS</td>
<td>27Jul15 06:15:12GMT</td>
</tr>
<tr>
<td>28/07/2015</td>
<td>Top rack</td>
<td>22.00</td>
<td>65.40</td>
<td>TS</td>
<td>28Jul15 06:23:25GMT</td>
</tr>
<tr>
<td>29/07/2015</td>
<td>Bottom rack</td>
<td>21.00</td>
<td>53.80</td>
<td>TS</td>
<td>29Jul15 06:07:10GMT</td>
</tr>
<tr>
<td>30/07/2015</td>
<td>Top rack</td>
<td>20.00</td>
<td>55.10</td>
<td>TS</td>
<td>30Jul15 06:04:30GMT</td>
</tr>
</tbody>
</table>

Available through the audit trail.
### Ditto, blank and brackets

<table>
<thead>
<tr>
<th>Date</th>
<th>Location As per WI023/1</th>
<th>Temp. &lt; 25°C</th>
<th>% RH &lt;75%</th>
<th>Operator</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/07/2015</td>
<td>Top rack</td>
<td>22.00</td>
<td>69.80</td>
<td>TS</td>
<td></td>
</tr>
<tr>
<td>21/07/2015</td>
<td>Top rack</td>
<td>23.00</td>
<td>68.30</td>
<td>&quot;</td>
<td></td>
</tr>
<tr>
<td>22/07/2015</td>
<td>Top rack</td>
<td>24.00</td>
<td>66.50</td>
<td>&quot;</td>
<td></td>
</tr>
<tr>
<td>23/07/2015</td>
<td>Bottom rack</td>
<td>25.00</td>
<td>62.10</td>
<td>&quot;</td>
<td></td>
</tr>
<tr>
<td>24/07/2015</td>
<td>Top rack</td>
<td>25.00</td>
<td>63.60</td>
<td>&quot;</td>
<td></td>
</tr>
<tr>
<td>27/07/2015</td>
<td>Top rack</td>
<td>25.00</td>
<td>75.90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28/07/2015</td>
<td>Top rack</td>
<td>22.00</td>
<td>65.40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29/07/2015</td>
<td>Bottom rack</td>
<td>21.00</td>
<td>53.80</td>
<td>TS</td>
<td></td>
</tr>
<tr>
<td>30/07/2015</td>
<td>Top rack</td>
<td>20.00</td>
<td>55.10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Functional verification vs validation?
Determined by system complexity

- Raw data includes equipment printouts, original workbook and logbook entries, readings transcribed by an operator from an electronic display, or a hand worked calculation, an observation etc.
- Raw data is a type of record but there is also an inference that the original 'result' is used further to derive a final result.
- Information captured within a batch record is raw data if it can’t be sourced from a validated electronic system.
### MHRA GMP Data Integrity Definitions & Guidance for Industry, March 2015 and Blog

<table>
<thead>
<tr>
<th>Compliment</th>
<th>PQS</th>
<th>Risk</th>
<th>Expectation</th>
<th>Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended to <strong>compliment</strong> existing EU GMP</td>
<td>The “data governance system” integral to the PQS</td>
<td>Effort and resource assigned to governance should be commensurate with the <strong>risk to product quality</strong></td>
<td>Not expected to implement a forensic approach</td>
<td>Design and operate a system that provides an acceptable state of control based on data integrity risk</td>
</tr>
</tbody>
</table>

**Data integrity requirements apply equally to manual (paper) and electronic data**
Data must be:

1. **A** – Attributable to the person generating the data
2. **L** – Legible and permanent
3. **C** – Contemporaneous
4. **O** – Original record (or “true copy”)
5. **A** – Accurate
## Design DI into your systems

### Paper based

<table>
<thead>
<tr>
<th>Attributable</th>
<th>Legible/Permanent</th>
<th>Contemporaneous</th>
<th>Original</th>
<th>Accurate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initials &amp; Signature registers</td>
<td>Control of blank forms, pen policy/white out</td>
<td>Documents available in right place at right time, +--time limits</td>
<td>Verified ‘true copies’, scans</td>
<td>Reflective of the observation data checking</td>
</tr>
</tbody>
</table>

#### Paper based

- **Active directory, e-sig, audit trails, metadata**
  - Data annotation tools, audit trail
  - System clock, sync., transaction window
  - Meta data, data about the data that permits reconstruction
  - Data capture, manual data entry

#### Electronic

**Slide 25**

© PharmOut 2015
**Take home message**

- It’s a big old problem
- Identify critical data
- It's not just the labs
- It’s not just IT systems
- Culture –
  - awareness and education

….. some basic behavioural, procedural and technical steps to significantly improve their systems.

MHRA – David Churchward
Thank you for your time.

Trevor Schoerie

trevor.schoerie@pharmout.net

www.pharmout.net