Medicines & Healthcare products Regulatory Agency

MHRA

Implementation of Data Integrity Guidance Requirements

Jason Wakelin-Smith, Lead Senior GCP & GLP Inspector

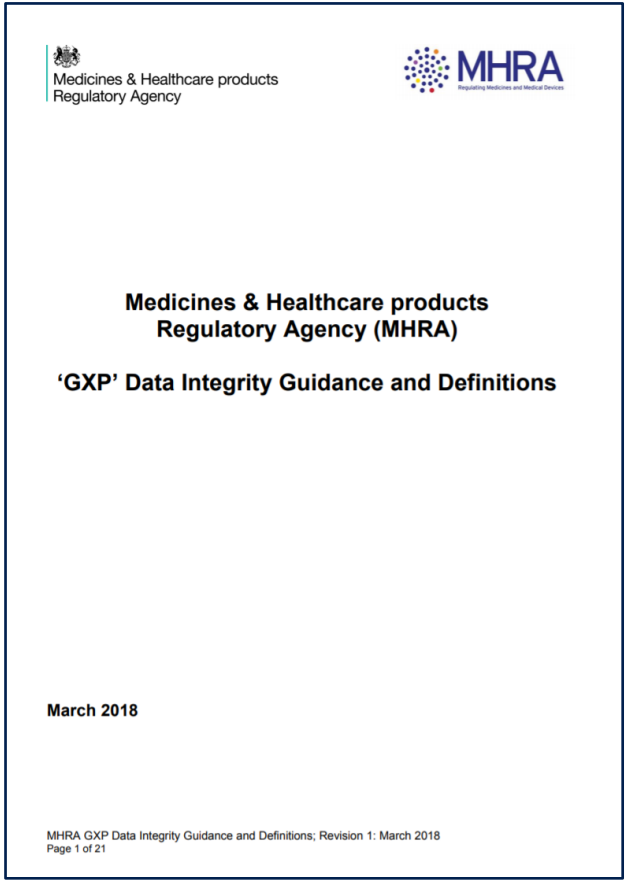


A Quick Fix?

- Understand the basics!
- Understand the terminology!

- Organisation-wide implementation required
- Cultural challenge
- Technical challenge
- Potentially significant changes ahead

- Multi-disciplinary input required
- Management input required


Medicines & Healthcare products Regulatory Agency

MHRA

Medicines & Healthcare products Regulatory Agency (MHRA)

'GXP' Data Integrity Guidance and Definitions

March 2018

MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018
Page 1 of 21

Data Integrity - Concepts

Data lifecycle - “All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, retention, archiving, retrieval and destruction”

Data Integrity - Concepts

Data Governance – "The sum total of arrangements to ensure that data irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle."

Data Governance

- Process & Systems
- Ownership
- Monitoring/Audit
- Environment
- Training

Define Your ‘Universe’

(AKA an Exercise in Process Mapping)

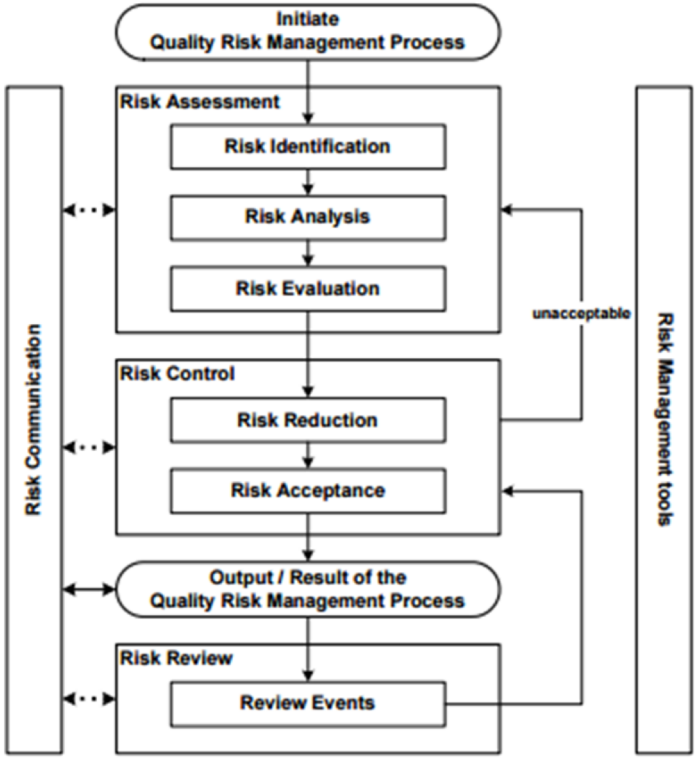
A Complicated Picture?

Next Steps

Understand the use of your data at each step in the map:

- What is the data used for?
- What existing controls exist?
- What oversight measures exist?
- What potential risks exist?
- Rationale for the decisions made?

Critical Data?



Not all data is equal!

Data criticality is determined by its intended use

Expectation that risk management principles used

Data Integrity Risk Assessment

Assessment of the vulnerability of the data to unintentional or unauthorised changes and the likelihood of detection

What can be done to mitigate the risks?

- Control measures
- Automation & validation
- Awareness of potential problem areas →increased scrutiny

Residual risks remain – how to acknowledge and control

Data Criticality Example

What is the data used for?

- Determining whether an analytical run is acceptable (e.g. QC values / calibration curve)

What existing controls exist?

- Defined acceptance criteria
- Defined analytical parameters
- Instrument settings defined in method

Data Criticality Example (2)

What oversight measures exist

- Analytical run review and management approval
- Audits

What potential risks exist?

- Sample manipulation
- Multiple sample acquisitions
- Integration parameters altered (impact on calibration curve)
- Data transfer (selection of results vs automated transfer)

Data Criticality Example (3)

Rationale

- QA have access to raw data & appropriate training
- Independent data review and approval
- No selection of results as automated transfer
- Audit trails
- Instrument permission settings
- Acceptance that data integrity measures are unlikely to stop someone who is determined to falsify data but they should make it much harder to do and easier to detect

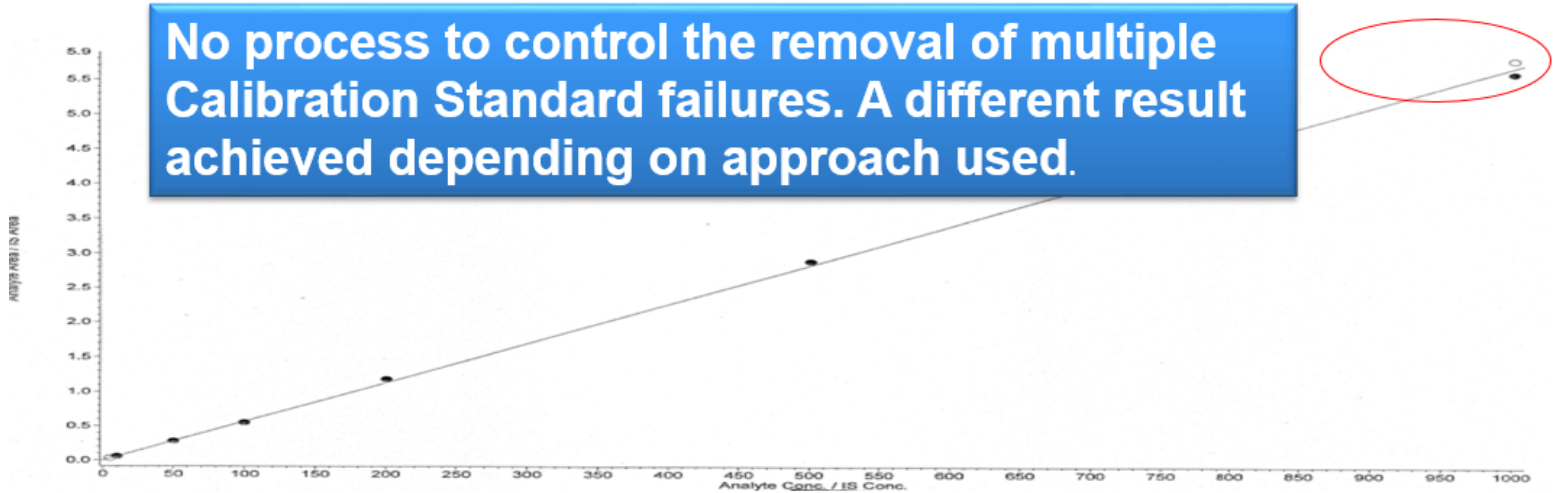
Audit Trail Considerations

- Know what audit trails exist and what they cover
- Understand what is ’normal’
- Understand the system terminology

- Data Integrity expectations – not a forensic approach
- ? Review by exception
- ? Targeted review based on run and study data

- If only audit the audit trail – then are you too late?

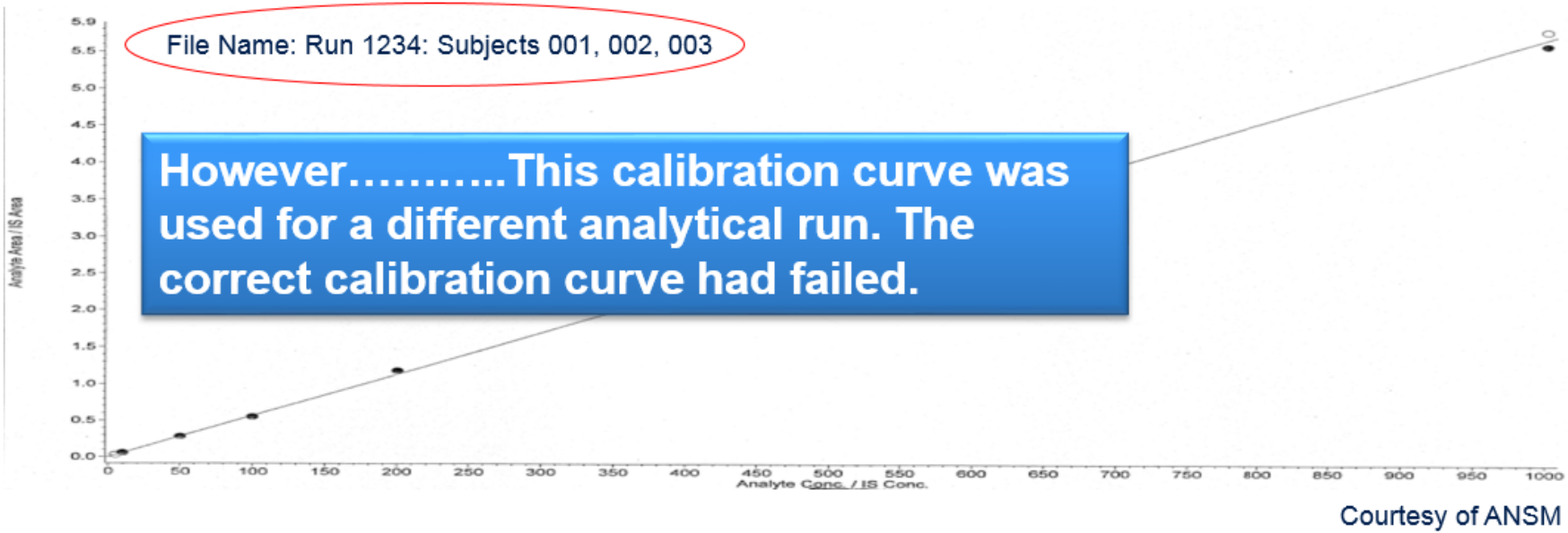
Food for Thought: Cals and QCs (1)



How is this controlled?

How would you know what approach was used?

Food for Thought: Cals and QCs (2)



Courtesy of ANSM

Would your systems and processes permit or identify this?

‘Red Flags’

- Controls not activated
- Stand alone systems
- Manual data recording
- Local data storage
- Manual data transfers
- ‘Opaque’ data
- Shared log-ins

Quality Assurance

To include assessment of both technical and GCP aspects

QA Staff

- Knowledge
- Access
- Time / people
- Control step in the process!
- Report?

Trying to avoid this…

None of the instruments or associated software within the laboratory had been configured to enable individual user accounts and to ensure appropriate data integrity controls.

- The software version used did not permit access to the ‘User Set Up’ functions stating that this functionality was only ‘available in the secure edition of the software’. This indicated that functionality to control individual user permissions was available within the software albeit in an additional module.
- The Scientist was both an analyst using the analyser and the system administrator with full rights to modify users and instrument settings.

Trying to avoid this (2)

- Analysts using the computer associated with the system had access to the Windows folder where CSV files containing the acquired analytical data would be stored. It would therefore be possible to manipulate and resave this data outside of the instrument software.
- The software version used with the instrument gave the user the option of turning off the connection to the LIMS and to amend the folder where the data for uploading would be found. It was therefore possible for the analyst to stop the upload, amend or replace the dataset and then upload to LIMS.
- It was possible to change the system date and time settings

Medicines & Healthcare products
Regulatory Agency

MHRA

Any Questions?

© Crown copyright 2018