MHRA Data Integrity Guidance and Expectations Document

Nichola Stevens – Alere International

John Andrews – Integrity Solutions

About this Session

This is an interactive session! We want you all to participate and share your thoughts on this guidance:

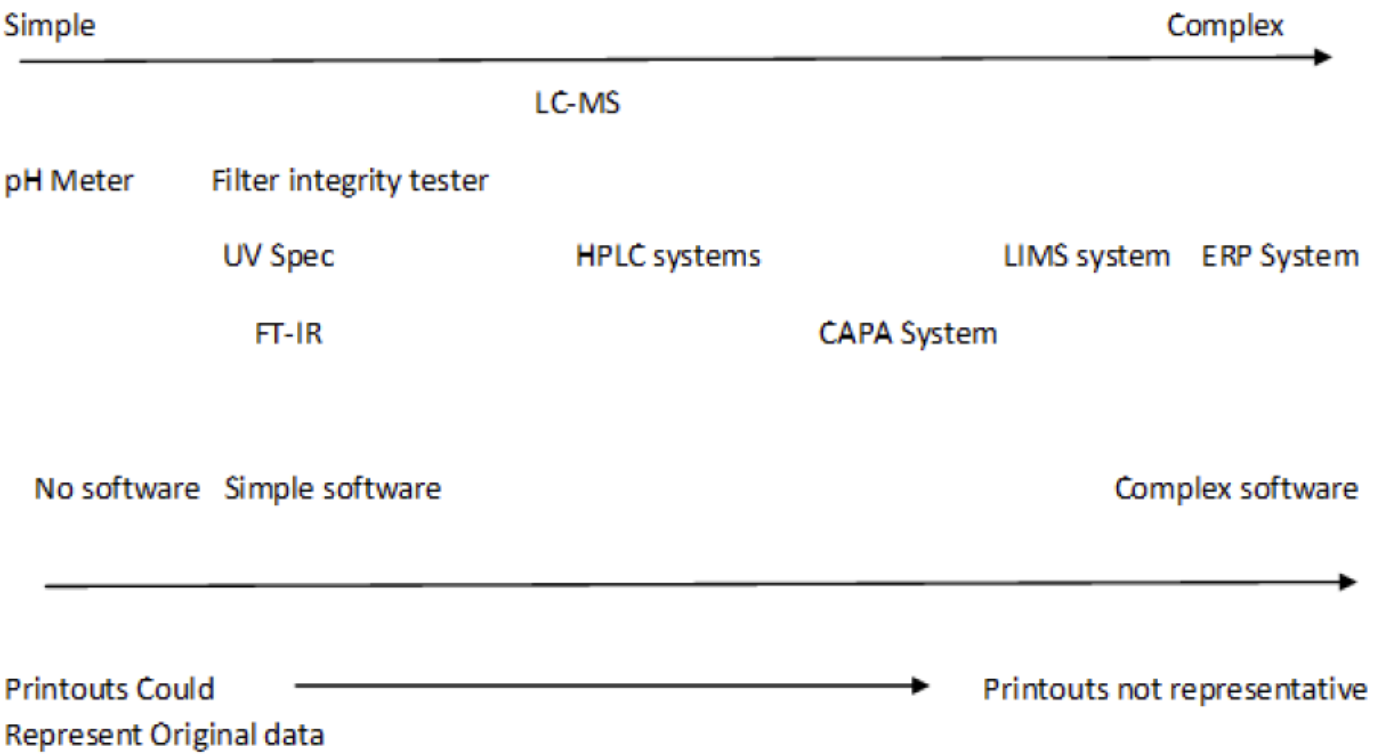
- Are there areas where it will be difficult to comply?
- Are there areas where more information is needed?
- Are there areas where the guidance doesn't go far enough?

Overview

- **MHRA GMP Data Integrity Definitions and Guidance for Industry**
- Published March 2015
- “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.”
- “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 a forensic 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.”

How relevant is this diagram? Would it be better to have a diagram which shows an ascending scale of risk to patient safety (e.g. QC systems more risk than those controlling manufacturing, etc)?

Figure 1: Diagram to illustrate the spectrum of simple machine (left) to complex computerised system (right), and relevance of printouts as 'original data'



The guidance says:

"The inherent risks to data integrity may differ depending upon the degree to which data (or the system generating or using the data) can be configured, and therefore potentially manipulated (see figure 1)."

Does more configuration mean greater risk of falsification or can it reduce the risk?

"It is common for companies to overlook systems of apparent lower complexity. Within these systems it may be possible to manipulate data or repeat testing to achieve a desired outcome with limited opportunity of detection."

Is this always true? Often the simple systems (e.g. balance or pH meter) are at the start of the process; is it may be easier/less time consuming to manipulate data further downstream in the process?

Designing systems to assure data quality and integrity

"Systems should be designed in a way that encourages compliance with the principles of data integrity. Examples include:

- Access to clocks for recording timed events
- Accessibility of batch records at locations where activities take place so that ad hoc data recording and later transcription to official records is not necessary
- Control over blank paper templates for data recording
- User access rights which prevent (or audit trail) data amendments
- Automated data capture or printers attached to equipment such as balances
- Proximity of printers to relevant activities
- Access to sampling points (e.g. for water systems)
- Access to raw data for staff performing data checking activities."

Anything else from an IT perspective?

Data Governance

MHRA Definition:

"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"

MHRA Expectation:

Data governance should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity including control over intentional and unintentional changes to information.

Questions:

- Do we know who owns the all the data within a computerised system?
- Could there be multiple owners?
- Where we are required to retain data for many years how good are we at maintaining ownership, especially as so many organisations are in a constant state of change?
- Suggestions for fully meeting this expectation?

Original record / true copy

MHRA Definition:

- **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 verified copy of an original record.
- Data may be static (e.g. a 'fixed' record such as paper or pdf) or dynamic (e.g. an electronic record which the user / reviewer can interact with).

MHRA Expectation:

- Many electronic records are important to retain in their dynamic (electronic) format, to enable interaction with the data. Data must be retained in a dynamic form where this is critical to its integrity or later verification. This should be justified based on risk.

Questions:

- Is it possible to keep records in a dynamic form for their entire lifecycle – this could be 30 + years?
- If not, at what point should we be thinking of moving from dynamic to something more static?

Audit Trail

MHRA Definition:

- GMP audit trails are metadata that are a record of GMP critical information (for example the change or deletion of GMP relevant data), which permit the reconstruction of GMP activities.

MHRA Expectation:

- The relevance of data retained in audit trails should be considered by the company to permit robust data review / verification. The items included in audit trail should be those of relevance to permit reconstruction of the process or activity. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.), and may be achieved by review of designed and validated system reports.

Questions:

- If only selected items in the audit trail need to be reviewed should this be included into the URS so that specific audit trail reports can be generated to facilitate review?

User Access / System Administrator Roles

MHRA Expectation:

- Full use should be made of access controls to ensure that people have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual . Companies must be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available.

Questions:

- What about access at the O/S or database level – how many of us are adequately controlling or recording this access?
- Are the risks at the O/S or database level less because those with access have no/less investment in the data?
- System Administrator activities should be audit trailed but how often / when should these activities be reviewed?

File Structure

MHRA Definition:

- Flat files: A 'flat file' is an individual record which may not carry with it all relevant metadata (e.g. pdf, dat, doc).
- Relational database: A relational database stores different components of associated data and metadata in different places. Each individual record is created and retrieved by compiling the data and metadata for review.

MHRA Comment:

- There is an inherently greater data integrity risk with flat files (e.g. when compared to data contained within a relational database), in that these are easier to manipulate and delete as a single file.
- A relational database file structure is inherently more secure, as the data is held in a large file format which preserves the relationship between data and metadata. This is more resilient to attempts to selectively delete, amend or recreate data and the metadata trail of actions, compared to a flat file system.

Questions:

- Is it really the case that a relational database is more secure – if I make a change within it will it be detected?
- If I make a change and it is detected does it automatically corrupt the data so that I can't use it?
- If so, is this any worse than deleting a flat file – I'm still without usable data?