HPRA

An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Electronic Systems - Regulators Observations

Catherine Neary

QP Forum

Trinity College Dublin, 16th April 2015

Agenda

- Introduction to Topic
- ‘Data Integrity’
- Considerations for any Electronic System
- Summary

Electronic Systems – Data Integrity
Annex 11, EU GMP Guide

Risk Management

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.

Electronic Systems – Data Integrity
Annex 11, EU GMP Guide

HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Data Storage

Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

Archiving

This data should be checked for accessibility, readability and integrity.

What is ‘Data Integrity’?

Data Integrity :-

- refers to **maintaining** and **assuring** the **accuracy** and **consistency** of data over its entire life-cycle and is a critical aspect to the design, implementation and usage of any system which stores, processes or retrieves data
- data is recorded exactly as intended, and upon later retrieval, the data is the same as it was when it was originally recorded
- data is complete, consistent & accurate

What is ‘Data Integrity’?

Data must be:-

A – attributable to the person generating the data

L – legible and permanent

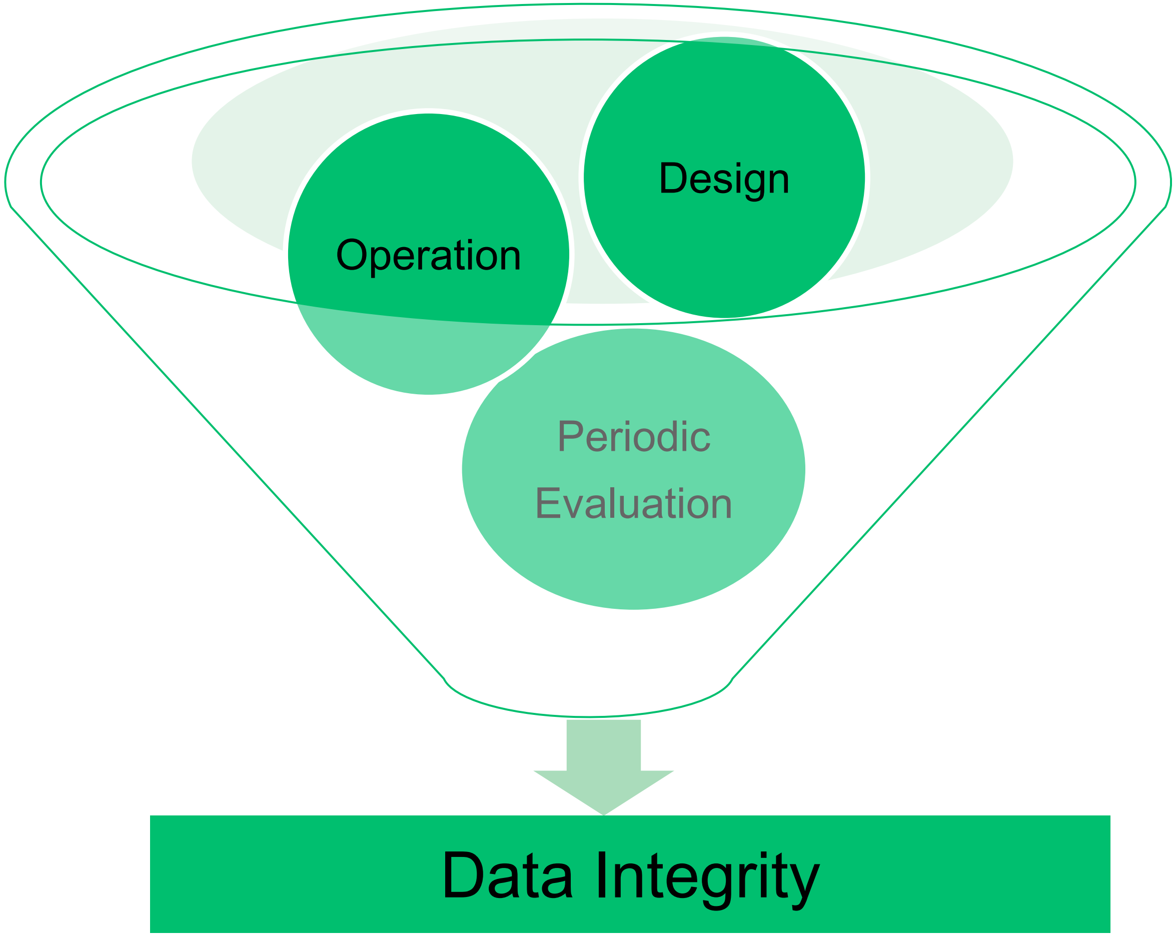
C – contemporaneous

O – original record (or ‘true copy’)

A – accurate

Electronic Systems

HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority



Design

Operation

Periodic Evaluation

Data Integrity

Design

- ➢URS
- ➢System Design
- ➢Security/access controls
- ➢Configuration settings
- ➢Audit trails
- ➢IT Infrastructure
- ➢Risk Management – extent & scope of validation & data integrity controls
- ➢Validation for intended us

Operation

- System operation
- Policies & Procedures
- Training
- Method/Recipe controls
- Generation/Processing of data
- Alarm management/reporting/review
- Review of data
- Approval of data
- Review of audit trails
- Records of checks

- Administrator privileges & access
- User privileges & access
- Back up
- Archiving
- Retrieval/restoration
- Documentation & investigation of data integrity breaches – deviations
- Deviation/CAPA /Risk management

Periodic evaluation

- Periodic evaluation & monitoring of system
- Review of audit trails
- Event logs/Helpdesk requests
- Self inspection (*involve the Subject Matter Experts & Administrators*)
- Change Management
- Risk Management
- Management of outsourced activities
- Business Continuity
- Continuous Improvement

Electronic Systems

Understand the system –

- ➢system complexity
- ➢configuration settings
- ➢access controls
- ➢data manipulation- which attributes may be altered?
- ➢audit trails

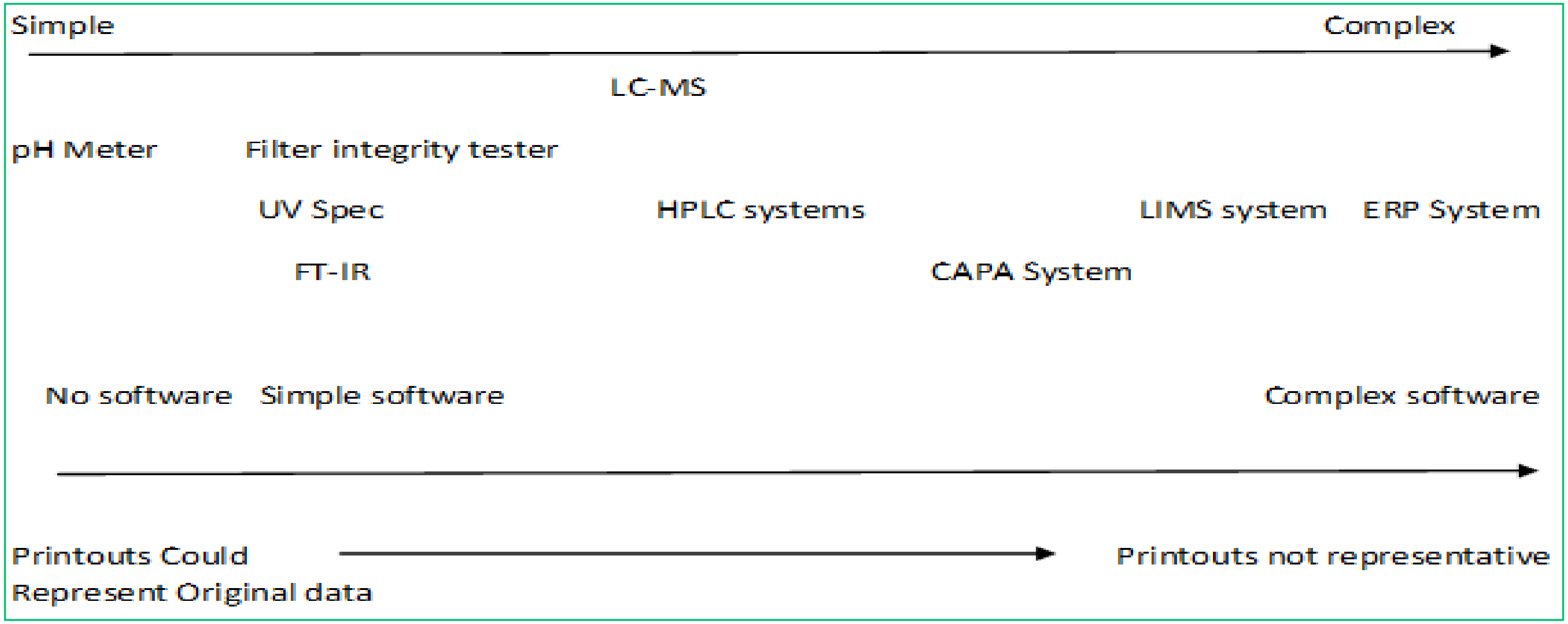
Risk assess the system & identify weaknesses -

- ➢data manipulation
- ➢repeat testing/runs
- ➢deletion
- ➢overwriting
- ➢date/time stamps

Identify & Implement measures to mitigate against the risks

Document rationale/justification in circumstances of risk acceptance

System Complexity



Simple

Complex

LC-MS

pH Meter

Filter integrity tester

UV Spec

HPLC systems

LIMS system

ERP System

FT-IR

CAPA System

No software

Simple software

Complex software

Printouts Could Represent Original data

Printouts not representative

(Diagram acknowledgement: Green Mountain QA LLC)

Article 23 of Directive 2001/83/EC

‘After a marketing authorisation has been granted, the marketing authorisation holder shall, in respect of the **methods of manufacture and control**.....**take account of scientific and technical progress** and introduce any changes that may be required to enable the medicinal product to be **manufactured and checked by means of generally accepted scientific methods**’

Summary

- The use of an electronic system does not reduce the requirements that would be expected for a manual system of data control and security.

- Prior to converting a process from manual to automated control (or the introduction of a new automated operation) it is important that company's consider **data integrity** as part of the impact assessment of risks.

  Risk reduction measures may need to be incorporated into the systems design and operation. (Additional risks to the quality of GxP related products/materials should not be introduced as a result of reducing the manual involvement in the process).

Regulatory References

- EU GMP Guide Annex 11:Computerised Systems (2011)

  http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf
- EMA Questions and Answers on EU GMP Guide Annex 11

  http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/general/gmp_q_a.jsp&mid=WC0b01ac058006e06c#section8
- PI 011-3 (2007) - PIC/S Guidance Good Practices For Computerised Systems in Regulated “GXP” Environments

  http://www.picscheme.org/pdf/27_pi-011-3-recommendation-on computerised-systems.pdf
- MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015

  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412735/Data_integrity_definitions_and_guidance_v2.pdf

Contact Details

Catherine Neary

Inspector

Health Products Regulatory Authority / An tÚdarás Rialála Táirgí Sláinte

Kevin O’Malley House, Earlsfort Centre, Earlsfort Terrace, Dublin 2.

Tel: +353 1 6764971

Fax: +353 1 6764061

catherine.neary@hpra.ie

www.hpra.ie