An Executive Summary

EDITORS' SERIES—
Addressing Data Integrity Gaps: Does Your Lab Have a Strategy?

Bob McDowall
Director
RD McDowall Limited

Understand the scope of a data integrity program and learn how to perform data process mapping on a chromatographic process.

Overview

Data integrity continues to be a major issue facing the pharmaceutical industry. Data integrity is not just a problem focused on computerized systems or on the laboratory, but also involves everyone in the organization from senior management down. This article provides an overview of which data integrity issues regulators are focusing on as well as guidance on how to map and manage data integrity processes and how to address data integrity gaps.

The Data Integrity Problem

Data integrity is a hot topic in the pharmaceutical industry and the focus of numerous warning letters. Guidance documents related to data integrity are available from numerous sources including the Food and Drug Administration (FDA), European regulators, the World Health Organization (WHO), the Pharmaceutical Inspection Cooperation Scheme (PIC/S), the International Society for Pharmaceutical Engineering (ISPE), the Parenteral Drug Association (PDA), and the European Compliance Academy.

Five new guidances were issued last year alone. Among the significant industry guidances are the ISPE Good Automated Manufacturing Practice Guidance, which is regarded as the definitive industry guidance on GxP computerized system compliance and validation, and the PDA Technical Report 80, which provides data integrity risks and the best practices that can be utilized to develop a robust data integrity management system to achieve compliance and mitigate risks (**Figure 1**).

Several key messages are indicated by the data integrity guidance documents. Among these are the reduction or elimination of paper records and hybrid systems in favor of electronic systems. For example, the guidance documents all refer to administrative controls for master templates and blank forms. For paper records, aligning with this aspect of the guidances can be onerous and impractical. With hybrid systems, linking and synchronizing two incompatible media is very difficult and second person review can be quite lengthy. The optimal approach is to implement electronic systems, through which data integrity can be ensured by implementing simple, elegant, streamlined workflows that are transparent and understandable, and by using technical controls built into the software, such as those to ensure there is no conflict of interest between the system administrator and system users. In addition, by implementing electronic signatures, the use of paper can be reduced and business processes can be streamlined.

Each of the individual data integrity guidances has additional key messages regarding the use of risk management to meet data integrity principles. For example:

- The WHO on Good Data & Record Management Practices (2016) refers to the need to map data processes and then apply risk management and sound science to defining the data lifecycle.

Figure 1: Data integrity guidance.

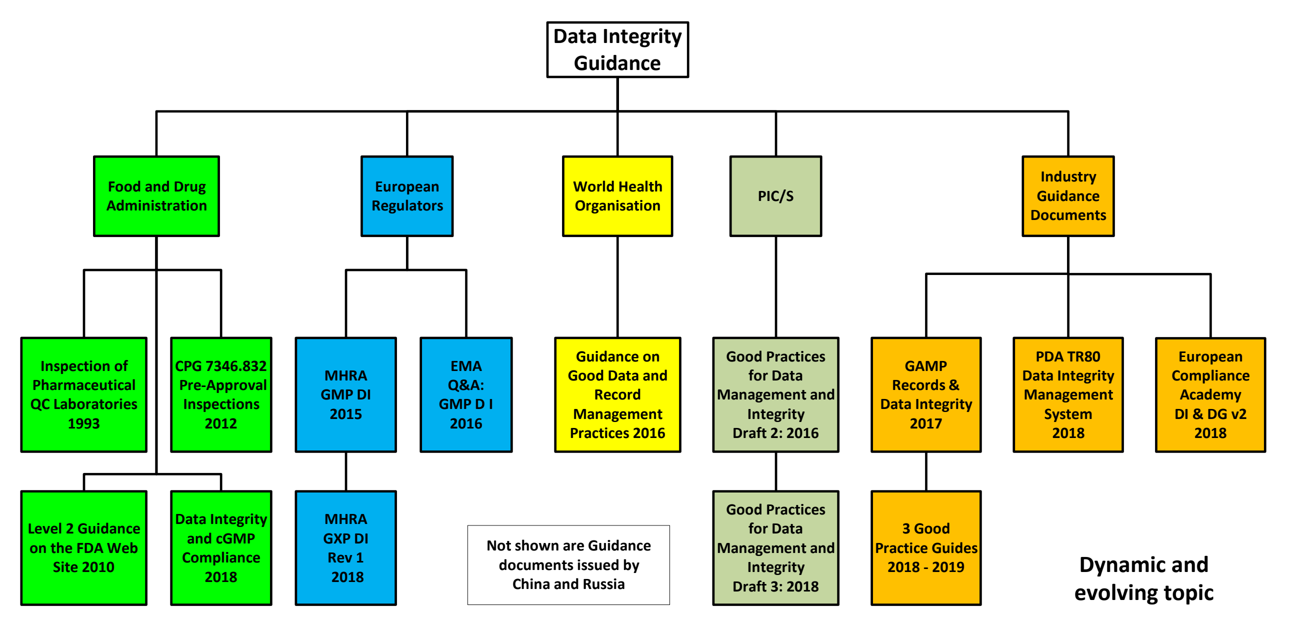

Data Integrity Guidance
Food and Drug Administration
European Regulators
World Health Organisation
PIC/S
Industry Guidance Documents
Inspection of Pharmaceutical QC Laboratories 1993
CPG 7346.832 Pre-Approval Inspections 2012
MHRA GMP DI 2015
EMA Q&A: GMP D I 2016
Guidance on Good Data and Record Management Practices 2016
Good Practices for Data Management and Integrity Draft 2: 2016
GAMP Records & Data Integrity 2017
PDA TR80 Data Integrity Management System 2018
European Compliance Academy DI & DG v2 2018
Level 2 Guidance on the FDA Web Site 2010
Data Integrity and cGMP Compliance 2018
MHRA GXP DI Rev 1 2018
Not shown are Guidance documents issued by China and Russia
Good Practices for Data Management and Integrity Draft 3: 2018
3 Good Practice Guides 2018 - 2019
Dynamic and evolving topic

Figure 2: Scope of data integrity.

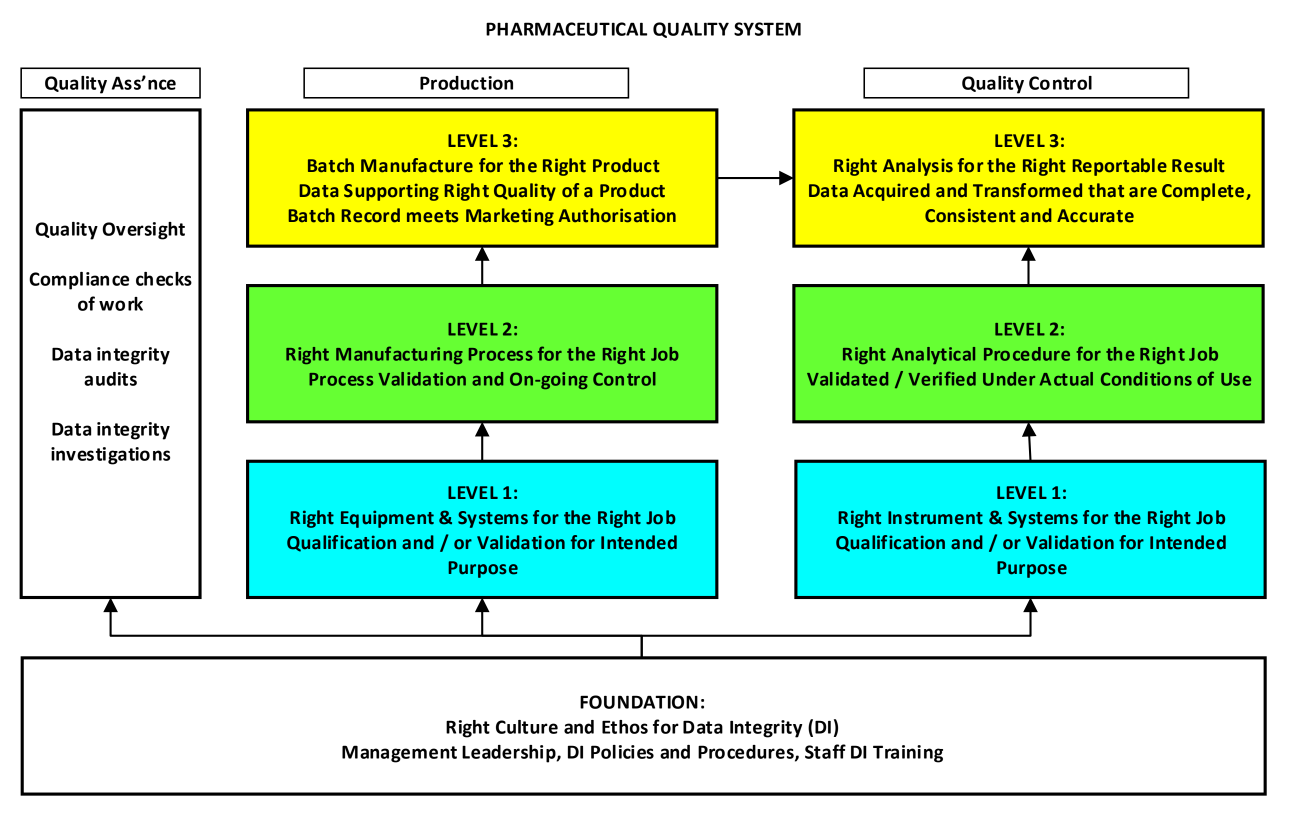
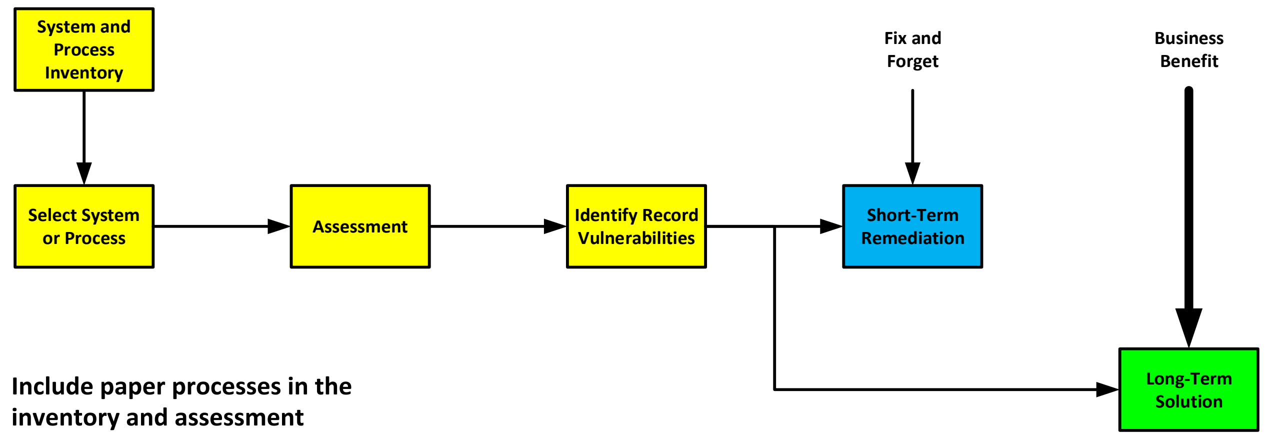

PHARMACEUTICAL QUALITY SYSTEM
Quality Ass'nce
Production
Quality Control
Quality Oversight
Compliance checks of work
Data integrity audits
Data integrity investigations
LEVEL 3: Batch Manufacture for the Right Product Data Supporting Right Quality of a Product Batch Record meets Marketing Authorisation
LEVEL 3: Right Analysis for the Right Reportable Result Data Acquired and Transformed that are Complete, Consistent and Accurate
LEVEL 2: Right Manufacturing Process for the Right Job Process Validation and On-going Control
LEVEL 2: Right Analytical Procedure for the Right Job Validated / Verified Under Actual Conditions of Use
LEVEL 1: Right Equipment & Systems for the Right Job Qualification and / or Validation for Intended Purpose
LEVEL 1: Right Instrument & Systems for the Right Job Qualification and / or Validation for Intended Purpose
FOUNDATION: Right Culture and Ethos for Data Integrity (DI) Management Leadership, DI Policies and Procedures, Staff DI Training

Figure 3: Assessment of processes and systems.


System and Process Inventory
Select System or Process
Assessment
Identify Record Vulnerabilities
Fix and Forget
Short-Term Remediation
Business Benefit
Long-Term Solution
Include paper processes in the inventory and assessment

- The PIC/S Good Practices for Data Management and Integrity (2018) refers to the use of risk management based on data criticality to determine the importance of each data/processing step.
- The Medicines and Healthcare Products Regulatory Agency (MHRA) "GXP" Data Integrity Guidance & Definitions (2018) refers to the need to operate a system with an acceptable state of control based on risk assessment.

In summary, the regulatory expectations are to map and understand data processes, to identify risks to the data that are generated, and to put controls in place to mitigate the risk.

Data Integrity in the Pharmaceutical Quality System

A useful model for interpreting the principles of data integrity provided in the regulatory guidances and for putting the principles into practice is provided in **Figure 2**. As illustrated, data integrity touches on all parts of the pharmaceutical quality system, which can be seen as having four levels.

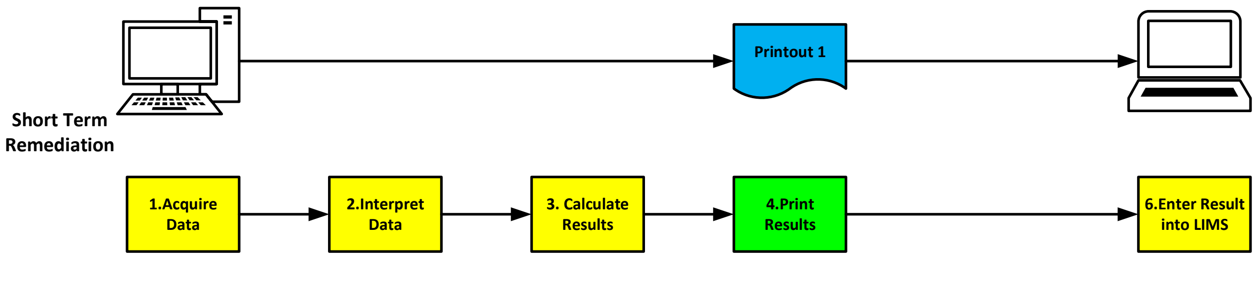
- The foundation level includes having the right culture and ethos for data integrity, as well as having management leadership that is involved. Management must get the culture and ethos right, raise problems, and admit mistakes.
- For the quality control pillar, directly above the foundation level in Level 1 is the need for the right analytical instruments and computerized systems to do the job and the requirement that these analytical instruments be qualified and that computer systems be validated for the intended use.
- Above that in Level 2 is the need for the right analytical procedure for the right job and requires that these procedures be validated or verified, as needed, to ensure that the procedures are under control.
- Above that in Level 3, which is dependent on the other three layers underneath, is the need for the right analysis for the right reportable result and the requirement that acquired and transformed data are complete, consistent, and accurate.

> "When it comes to assessing a laboratory with several stand-alone chromatography data systems (CDS), FDA 483 findings continue to reveal numerous vulnerabilities. It is not unusual to find that users share login credentials, so there is no means of attribution, and that they often have access to all of the administrative system privileges."

Assessment of Processes and Systems

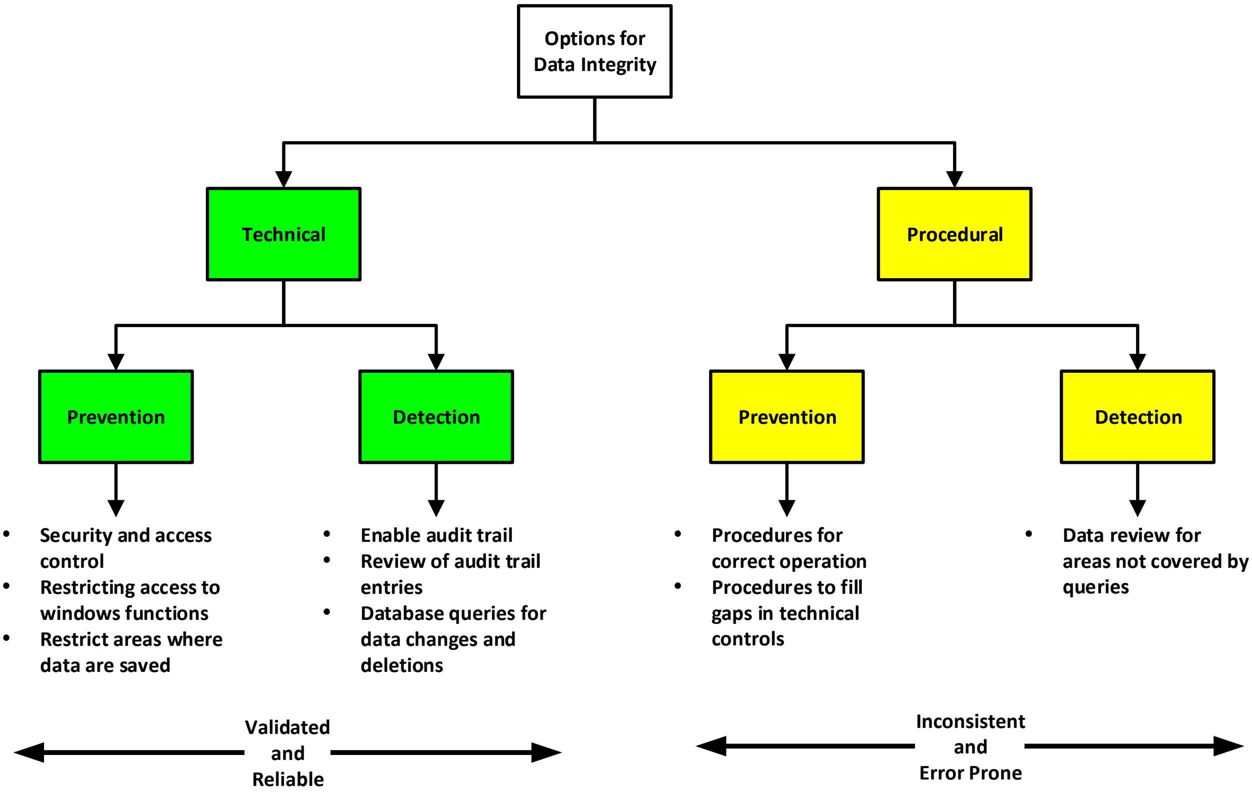
Compliance with the data integrity guidances starts with an assessment of processes and systems (**Figure 3**). The first step is to compile an inventory of paper-based, hybrid, and electronic processes and systems. Then, each system is assessed to identify vulnerabilities, starting with the most critical systems. There are two assessment approaches: use of a checklist or data process mapping. A checklist can be useful, but strict adherence to the checklist may result in risks being missed. Also, checklists tend to be used to assess computerized systems, while paper-based processes are often overlooked. On the other hand, data

Figure 4: Short-term remediation.



- Each user uniquely identified and given user role
- User roles remove conflict of interest: user from administration
- E-records and paper print outs are record set
- SOP for integration: key is when you can and can't manually integrate
- Spreadsheet exterminated – all calculations in CDS
- Job done?

Figure 5: Long-term vs. short-term remediation.



- Security and access control
- Restricting access to windows functions
- Restrict areas where data are saved

- Enable audit trail
- Review of audit trail entries
- Database queries for data changes and deletions

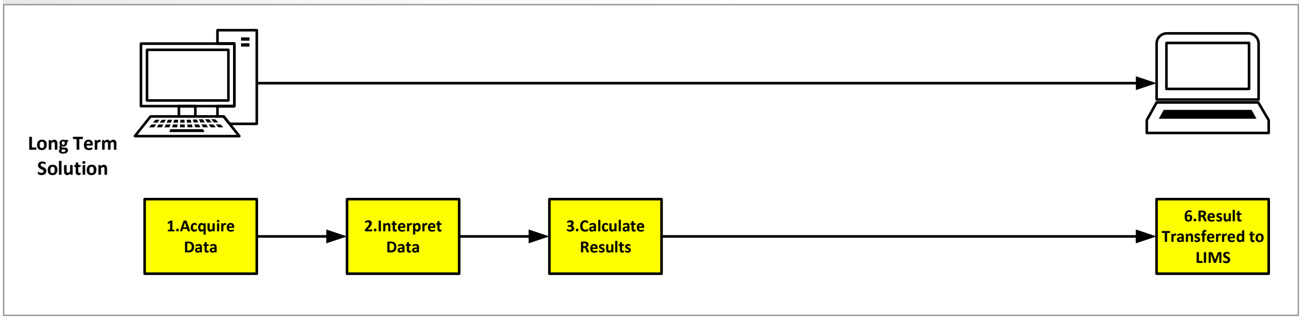
- Procedures for correct operation
- Procedures to fill gaps in technical controls

- Data review for areas not covered by queries

process mapping involving subject matter experts is more likely to provide visualization of the entire process, including all data and risks.

Data process mapping is commonly done using a whiteboard or a flip chart and involves a facilitator who works with subject matter experts that know the computer system and/or the manual processes that surround it. The facilitator asks straightforward questions like: What do you do? How do you start? What are the inputs? What do you do in this process? The process is iterative and it make take two or three attempts until the entire process can be visualized. Once completed, its advantage over checklists is the ability to see the entire

Figure 6: Business improvement.



process on a small number of pages, whereas a checklist require a large number of pages.

When it comes to assessing a laboratory with several stand-alone chromatography data systems (CDS), FDA 483 findings continue to reveal numerous vulnerabilities. It is not unusual to find that users share login credentials, so there is no means of attribution, and that they often have access to all of the administrative system privileges. For each stand-alone CDS, there must be a minimum of two roles: user and administrator. In addition, each user must have his or her own unique login credentials. Raw data is often in paper form. If electronic record backups are performed, there is often a variety of options (e.g., USB sticks and external drives) and backups are not always done on a routine basis. In the absence of proper technical controls, integration of chromatograms is performed manually and inconsistently, and peak areas are often entered manually into a nonvalidated spreadsheet. In many instances, audit trail functionality can be turned on and off at any time. All of these vulnerabilities can be remediated by interfacing the CDS with a Laboratory Information System (LIMS) and a network server.

Remediation of Data Integrity Vulnerabilities

There are two approaches that can be taken to address data integrity vulnerabilities: short-term remediation (**Figure 4**) and long-term solutions and strategy (**Figure 5**). The short-term approach involves the use of existing technical controls coupled with procedural controls. Long-term solutions involve validated technical controls and mapping of the data flow and will deliver a far more efficient process for identifying current and potential gaps. Short-term remediation can provide an immediate solution to a problem. However, short-term solutions, which typically involve the implementation of paper-based, procedural controls, can be relatively inefficient, inconsistent, and error-prone because such controls are performed by humans.

In contrast, long-term, validated technical solutions such as those involving electronic signatures and configuration controls for prevention of falsification and detection of falsification or poor data management practices are more reliable and more efficient, thereby providing a substantial business benefit. Common examples of the implementation of the realization of business improvement through the implementation of technical controls to address data integrity include interfacing a CDS with a LIMS and networking of formerly stand-alone CDS to a secure, validated network server. The implementation of these technical controls will enable automated backup of records, comprehensive audit trails, consistency of the application of chromatography methods, and, overall, a more efficient and effective business process (**Figure 6**).

Conclusion

Data integrity continues to be a major issue facing the pharmaceutical industry, as evidenced by the fact that FDA 483 findings continue to reveal numerous data integrity vulnerabilities. The numerous regulatory guidances on this topic indicate there are significant advantages to reducing or eliminating paper-based or hybrid systems and processes in favor of electronic systems. The technical controls available through these electronic systems will significantly improve compliance with data integrity regulations, while also providing the added benefit of efficient, streamlined business processes.