LCGC

Data Integrity in Regulated Laboratories

APRIL 2019

Understanding the Scope of Data Integrity
R.D. McDowall

Using Data Process Mapping to Identify Integrity Gaps
R.D. McDowall

What Is the Problem with Hybrid Systems?
R.D. McDowall

Sponsored by

Agilent

This custom ebook is sponsored by Agilent and presented in partnership with *LCGC*

Agilent OpenLab

Increase Productivity While Meeting Data Integrity Requirements

Upgrade to Agilent OpenLab CDS

Choosing the right data system can make all the difference. OpenLab CDS is a single, secure chromatography data system for chromatography and single-quadrupole MS workflows that enables you to streamline laboratory operations and efficiently generate quality results.

OpenLab CDS ensures data integrity and facilitates rigorous regulatory compliance with your choice of technical controls—such as audit trail review, access control, records protection, and e-signatures.

Learn more about Agilent OpenLab CDS.

www.agilent.com/chem/openlabcds-streamline

Agilent

485F US Highway One South, Suite 210,
Iselin, NJ 08830
(732) 596-0276

To subscribe, call toll-free 888-527-7008. Outside the U.S. call 218-740-6477.

LCGC North America (ISSN 1527-5949 print) (ISSN 1939-1889 digital) is published monthly by MultiMedia Healthcare LLC, 325 West First Street STE 300 Duluth, MN 55802, and is distributed free of charge to users and specifiers of chromatographic equipment in the United States and Canada.

INTRODUCTION

According to R.D. McDowall, director of RD McDowall Limited in the UK (1), "Data integrity requires more than just ensuring that the calculated numbers of an analysis are complete, consistent and accurate." Rather, laboratories have many aspects to consider that all fall under the umbrella of data integrity, from how to identify data gaps to taking the problems associated with hybrid computerized systems seriously.

These data integrity topics (plus many more) were covered in a recently published *LCGC North America* multipart series* authored by McDowall on "Data Integrity in Regulated Laboratories"; the first three articles in this six-part series are reprinted here.

Building on a previous discussion of data integrity (2), the first article explores a four-layer data integrity model that demonstrates the scope of a data integrity and data governance program. Next, McDowall discusses how data process mapping is a vital step for identifying data integrity gaps within chromatography data system processes. Here, he also explores ways to eliminate these gaps.

The third installment of this series focuses on hybrid computerized system, namely, what they are, why they are problematic, and what laboratories can do to transition to fully computerized systems.

References

1. R.D. McDowall, *LCGC North Am.* **37**(1), 44–51 (2019).

2. M.E. Newton and R.D. McDowall, LCGC North Am. **36**(5), 330–335 (2018).

*Parts IV–VI of this series will be presented in future issues of LCGC.

Understanding the Scope of Data Integrity

R.D. McDowall

Data integrity requires more than just ensuring that the calculated numbers of an analysis are complete, consistent and accurate. There is much more to consider. The full scope of a data integrity and data governance program can be presented and explained in a simple diagram.

Welcome to "Data Integrity Focus," a six-part series on data integrity in regulated laboratories that will also be of use to other readers working under quality standards such as ISO 17025 (1). We will explore some selected topics in data integrity and data governance. To begin, we will discuss the scope of a data integrity program.

Last year in *LCGC North America*, Mark Newton and I wrote a six-part series on data integrity in the regulated chromatography laboratory (2–7) in which we reviewed the whole analytical process. In Part 1, we introduced briefly a four-layer model to explain the scope of data integrity (3). In this first part of "Data Integrity Focus," I would like to go into more detail of the model so that you can understand the different strands of a data integrity program. Note the use of the word "program." Data integrity has many strands of work; it is not a single project. There are multiple projects that come under the umbrella of a program. Let me explain the data integrity model in more detail so that you can see why.

Data Integrity Within a Quality System

Over the past decade, pharmaceutical regulation has focused on the development of a pharmaceutical quality system (PQS) based on the ISO 9000 quality management system (QMS) following the publication of the International Council for Harmonization (ICH) Q10 guidance (8) and the update of EU GMP Chapter 1 (9). In a PQS, senior management have overall responsibility and accountability for all activities and data generated (8,9). Although data integrity has always been implicit in regulations, section 1.9 of EU GMP Chapter 1 was updated so that work performed by

Quality Control laboratories must proceed as follows:

> *"(iv) Records are made, manually and/or by recording instruments, which demonstrate that all the required sampling, inspecting and testing procedures were actually carried out. Any deviations are fully recorded and investigated (9)."*

Implicit in this definition is that the records generated have adequate quality and integrity. As an aside, EU GMP Chapter 4 on documentation and Annex 11 for computerized systems are being revised to emphasize data integrity (10).

Data Integrity Model

To understand the scope of data integrity, a four-layer model has been developed, covering development, production, quality control (QC), and quality assurance (QA). The full GMP model is discussed in my books (11,12) and the initial discussion of the analytical portion was presented in Spectroscopy (13). The four layers are shown in **Figure 1** and described below for a regulated laboratory and QA only:

Foundation: Right Corporate Culture for Data Integrity

The foundation goes across all elements in an organization and is the data governance layer. The elements here for data integrity are management leadership, data integrity policies including data ownership, staff training in these procedures, management review including quality metrics and the establishment, and maintenance of an open culture with ethical working by all staff.

Level 1: Right Instrument or System for the Job

Analysis requires analytical instruments and computer applications to ensure data quality, and data integrity instruments must be qualified and software including spreadsheets must be validated. Included here are calibration, point-of-use checks, or system suitability test samples to confirm that the analytical instrument or laboratory computerized system is within user specifications before use.

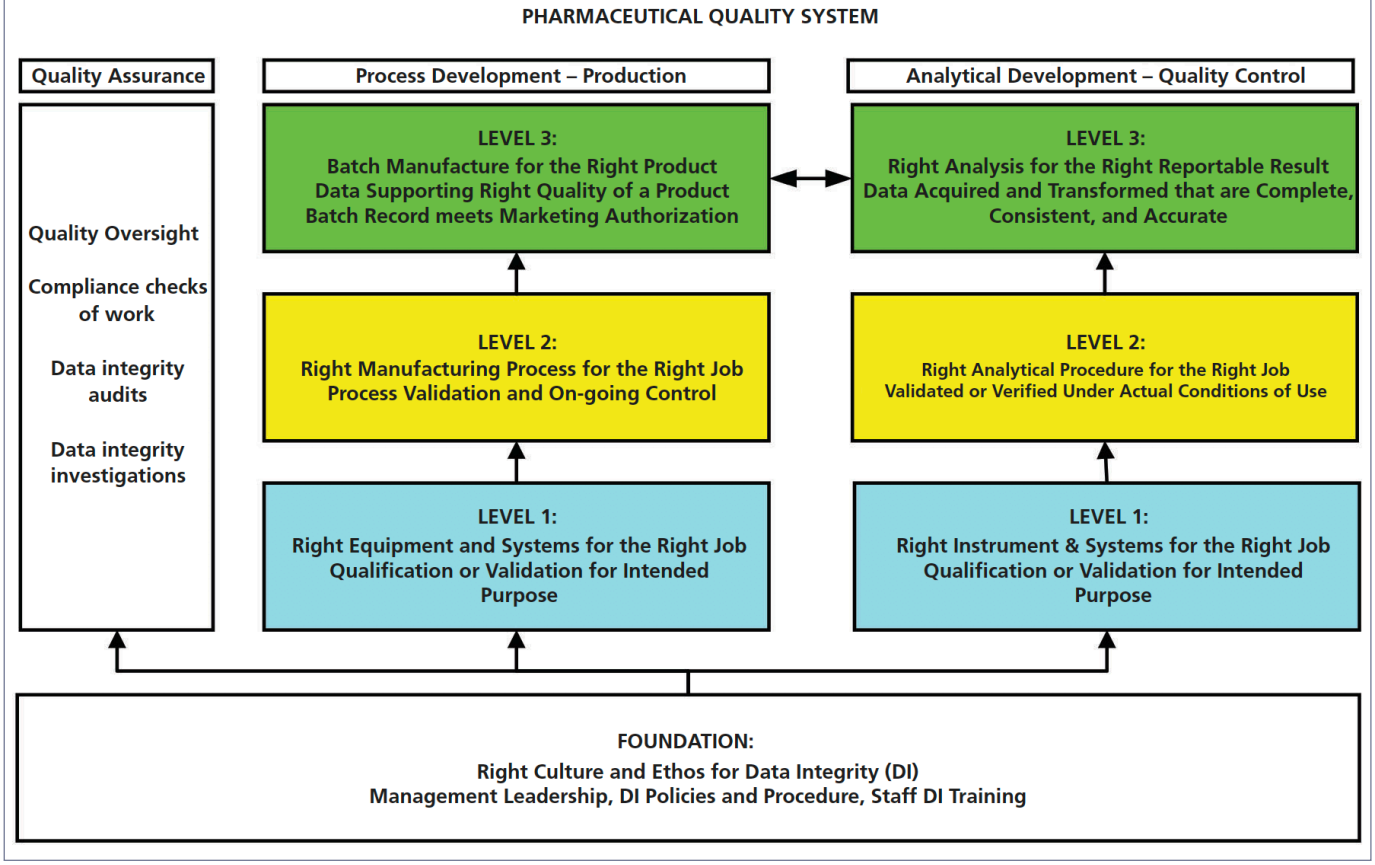
Level 2: Right Analytical Procedure for the Job

For a laboratory, this is validation or verification of analytical procedures under actual conditions of use. What is not covered in current regulations or guidance is method development, which will determine the robustness of the procedure; this is the subject of a draft *United States Pharmacopeia* (*USP*) general chapter <1220> (14) on analytical procedure lifecycle management (APLM).

Level 3: Right Analysis for the Right Reportable Result

Here, process development and production provide the laboratory samples for analysis that are taken to demonstrate adequate product quality and conformance with the product specification in the marketing authorization (MA). It is this level where the work of the three layers below is essential

Figure 1: A Data Integrity Model. Reproduced with Permission from The Royal Society of Chemistry (11).



for work to be performed ethically and correctly and where deviations occur they are investigated (9).

Quality Oversight

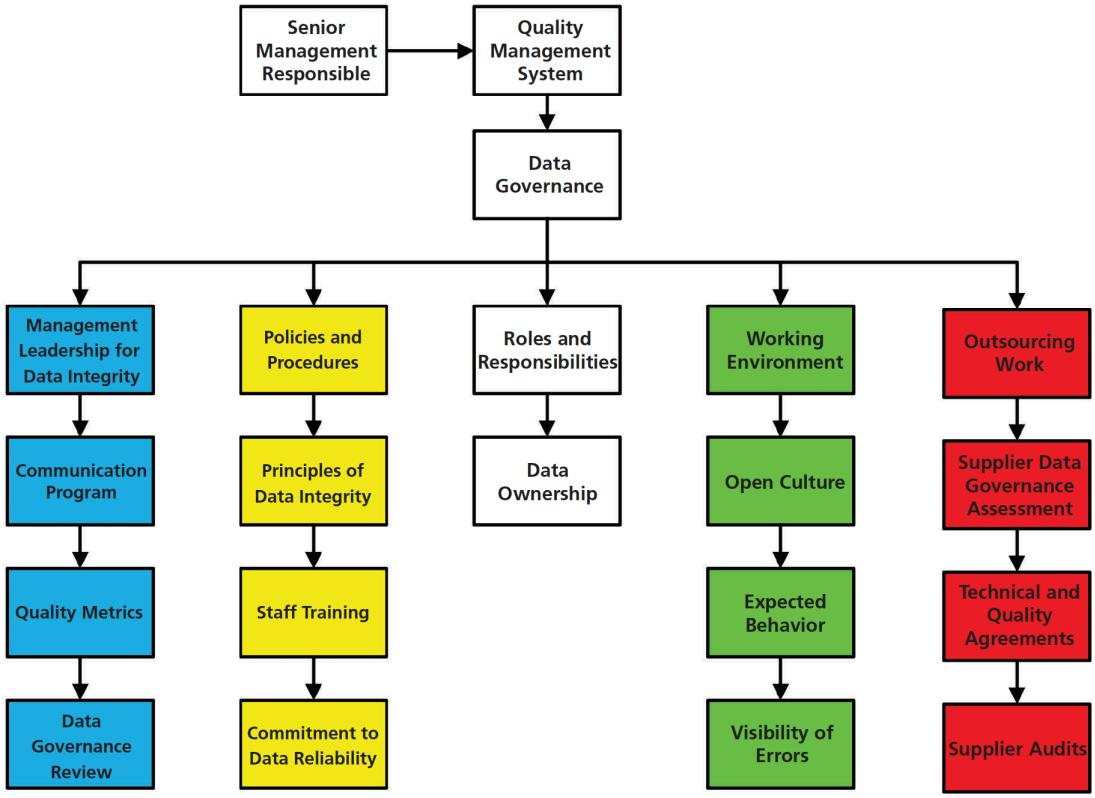
Although shown on the left of Figure 1 because of the sample link between production and quality control, the QA function is pervasive throughout the data integrity model to provide quality oversight of both production and laboratory operations, such as ensuring compliance with regulations, policies, and procedures as well as performing data integrity audits and data integrity investigations.

This is an overview of the data integrity model. We will now look in more detail at each level of the model for a regulated laboratory.

Foundation Level: Data Governance

The first level is called the *Foundation Level* for a very specific reason: Data integrity and data governance start with senior management involvement. Without it, any work at the levels above will be wasted. As shown in **Figure 2**, the Foundation Level has several elements that are essential for data integrity, which are explained below.

Figure 2: Data governance functions at the foundation level. Adapted from reference (11) with Permission.



Management Leadership and Involvement with the PQS

- Senior management leadership for data integrity that includes a communication program for all staff about the importance of data integrity and the impact it can have on patients and the organization if instances of noncompliance are found.
- Generation and use of quality metrics for monitoring data integrity. This is the subject of the two papers by Newton and McDowall (7,15) and will not be discussed further here.
- As part of the Pharmaceutical Quality System, a review of the effectiveness of the data governance and data integrity projects within the overall program. EU GMP Chapter 1 (9) mandates that management must review the QMS and data integrity is part of that review process.

Policies and Procedures Need to Be in Place, Including:

- Writing a data integrity policy with initial and ongoing training in its contents. After being trained, all members of staff should sign a commitment to data reliability for their work. Although the EMA

Q&A (16) notes that there is no regulation for a data integrity policy, guidance documents issued by the Medicines and Healthcare Products Regulatory Agency (MHRA), the World Health Organization (WHO), and the Pharmaceutical Inspection Co-operation Scheme (PIC/S) guidances (17–21) all note that one is needed.

- Good documentation practices covering paper, hybrid, and electronic processes coupled with training in the procedure. This should include defining a flexible analytical data life cycle that was discussed in a recent column (22) with more detail of this approach in my book (11).
- Interpretation of analytical data, such as chromatographic integration, comparison of spectra using libraries, what are analysts allowed to do, and when and what specifically activities are prohibited.
- Training in these procedures with demonstrable understanding of the contents evidenced by using questionnaires or practical execution of the procedure.

Who Does What?

- The roles and responsibilities of all staff involved in a data governance and data integrity program including data ownership need to be documented and the information transmitted to all staff (11).
- Roles and responsibilities must be reinforced by appropriate sections in each individual's job or position description.
- Incorporation of data integrity goals into personnel objectives must be completed.

Quality Culture and the Working Environment

- Senior management needs to create an open quality culture where there are standards for expected behavior. This is probably the most difficult task in the whole data integrity program: It does not consist of a single e-mail, but an ongoing task to affect a culture change in an organization. It is not an event but a journey. ISPE has published a Cultural Excellence report (23) and there is also an abridged section on corporate culture in the recent *GAMP Good Practice Guide on Data integrity – Key Concepts* (24).
- Gemba walks where management gets to see issues in the laboratory first hand rather than filtered by subordinates (23). It is also an opportunity to influence staff directly by promoting the open culture and owning up to mistakes.
- Accordingly, there is an expected behavior and an open culture where mistakes can be admitted without blame. Admitting mistakes is also a regulatory expectation as noted in the Analyst Responsibilities section of the FDA OOS Guidance (25) that states:

  "If errors are obvious, such as the spilling of a sample solution or the incomplete transfer of a sample composite, the analyst should immediately document what happened. Analysts should not knowingly continue an analysis they expect to invalidate at a later time for an assignable cause (i.e., analyses should not be completed for the sole purpose of seeing what results

can be obtained when obvious errors are known)."

Outsourcing Work

- Any outsourced work requires an assessment of the outsourcing organization's or laboratory's data governance and data integrity status before technical and quality agreements are written and signed.

Level 1: Integrated Instrument Qualification and Computer Validation

There is little point in carrying out an analysis if an analytical instrument is not adequately qualified, or the software that controls it or processes data is not validated. Therefore, at Level 1, the analytical instruments and computerized systems used in the laboratory must be qualified for the specified operating range, and validated for their intended purpose, respectively. There are the following sources:

- *USP* <1058> for Analytical Instrument Qualification, 2018 version (26)
- *GAMP Good Practice Guide for Validation of Laboratory Computerised Systems,* 2nd Edition (27)
- *Validation of Chromatography Data Systems,* 2nd Edition (12)

These documents provide guidance and advice on these two interrelated subjects. Indeed, the new version of *USP* <1058> integrates instrument qualification and computer validation for analytical equipment (26) and the integrated approach is discussed in more detail in recent publications (12,28–30) A user requirements specification must be written for both instruments and software to define the intended use and against

"There is little point in carrying out an analysis if an analytical instrument is not adequately qualified, or the software that controls it or processes data is not validated."

which the instrument will be qualified and the software validated. Where the software application must be configured to protect electronic records generated by the system, this must be reflected in the validation documents for the application software. By implementing suitable controls to transfer, mitigate, or eliminate any record vulnerabilities so that they can be adequately protected and ensure data integrity. Burgess and McDowall in an earlier *LCGC* series about an ideal chromatography data system (CDS) discussed some of the architecture, workflow and compliance requirements for ensuring data integrity (31–34).

Failure to ensure that an analytical instrument is adequately qualified or software is adequately validated means that all work in the top two levels of the data integrity model is wasted, as the quality and integrity of the reportable results is compromised by unqualified instrumentation and unvalidated and uncontrolled software.

Assessment, remediation, and long-term solution of paper processes and computerized systems are also included in this level of the model.

Level 2: Analytical Procedure Lifecycle Management

Using qualified analytical instruments with validated software, an analytical procedure is developed or established, and then validated or verified. The GMP requirement is that analytical methods must be verified under actual conditions of use as per 21 *CFR* 211.194(a)(2) (35), and, therefore, be fit for its intended use.

There are several published references for method validation from ICH Q2(R1) (36), FDA validation guidance documents (37,38) and the respective chapters in the *European Pharmacopoeia* (EP) and *United States Pharmacopoeia* (USP). However, the focus of these publications is validation of an analytical procedure that has been already developed. Method development is far more important, as it determines the overall robustness or ruggedness of any analytical procedure, but this process receives little or no attention in these publications. However, this analytical world is changing; following the publication in 2012 by Martin et al (39), there is a draft *USP* <1220> on The Analytical Procedure Lifecycle (14), issued for comment. This will mean a move from chapters focused only on validation, verification, or transfer of a method to a life cycle approach to analytical chapters that encompass development, validation, transfer, and continual improvement of analytical methods.

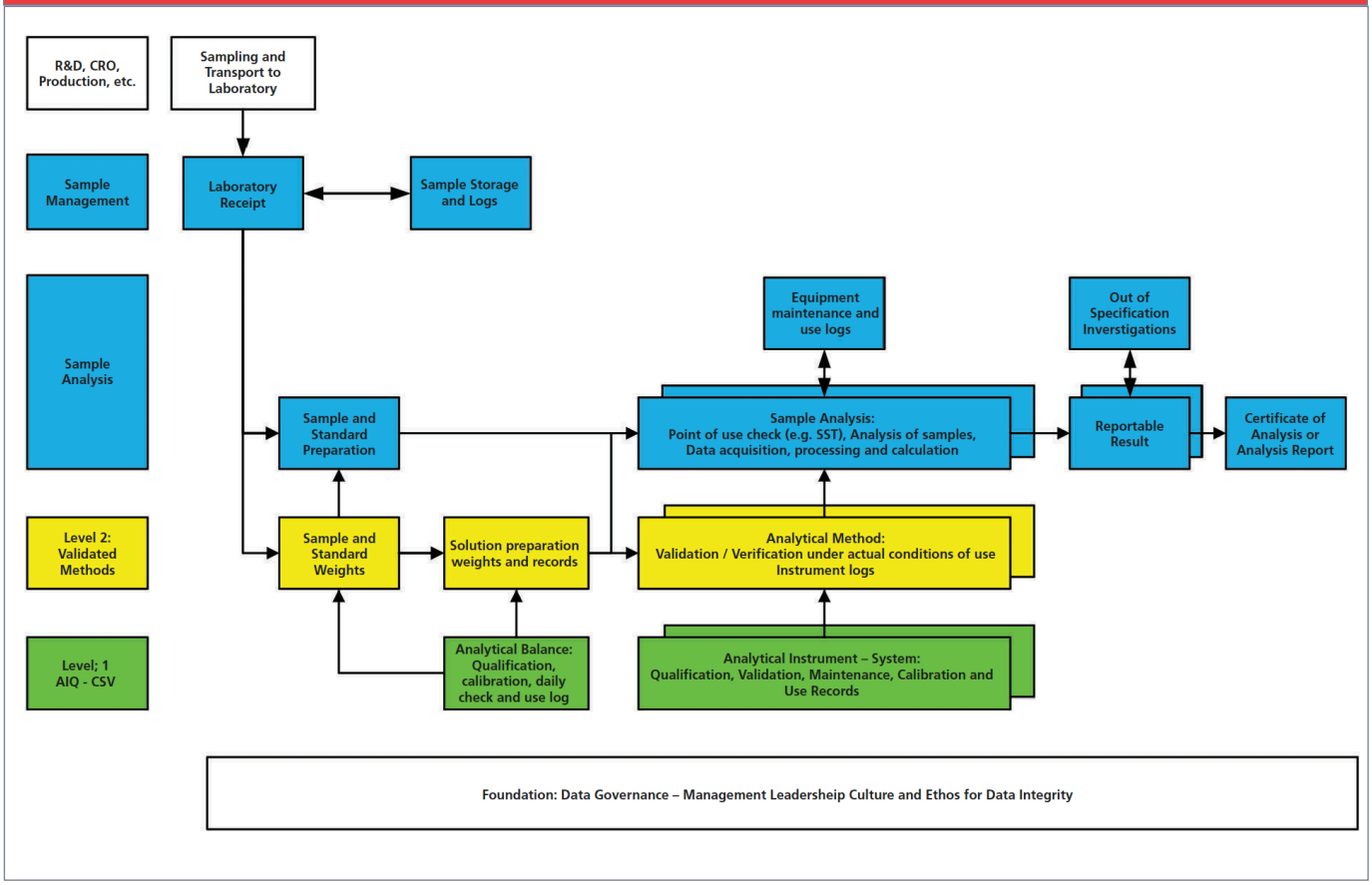
A life cycle approach to analytical procedures validation means that definition of an Analytical Target Profile (ATP) leads to good scientifically sound method development that ends with the definition of the procedure's design space, which now becomes important, as changes to a validated method within the validated design space would be deemed to be validated per se. There will be a transition period where the old approach is phased out while the new one is phased in. There is currently an ICH initiative that began in 2018 to update ICH Q2(R1) (36) to a life cycle approach (40).

"A life cycle approach to analytical procedures validation means that definition of an Analytical Target Profile (ATP) leads to good scientifically sound method development that ends with the definition of the procedure's design space."

Verification of Pharmacopoeial Methods

Given the vague descriptions of most analytical methods in various pharmacopoeias, it is amazing that any laboratory can get a method working at all. In essence, pharmacopoeial methods are unlikely to work as written. One of the reasons is that if a method for high performance liquid chromatography (HPLC) is developed using a specific supplier's C18 column, the only information about

Figure 3: Interaction of the four levels of the data integrity model. Adapted with permission from reference (11). Definition of acronyms: Research and development (R&D), contract research organization (CRO), analytical instrument qualification (AIQ), computerized system validation (CSV), and system suitability test (SST).



the column that appears in the monograph is a description of the packing and the column dimensions. For gradient methods, there is no information about whether the gradient is formed using a low-pressure or high-pressure mixing pump. For these reasons, analytical procedures based on pharmacopoeial "methods" need to be developed and verified under actual conditions of use as required by 21 *CFR* 211.194(a)(2) (35). The pharmacopoeia simply provides an indication of where to start but the details are left to the individual laboratory to develop, document, and verify.

Level 3: Analysis of Samples

Finally, at Level 3 of the data integrity model, the analysis of sample will be undertaken using the right analytical procedure, using a qualified analytical instrument and processing with validated software applications. To be successful, this also requires an open environment that enables data to be generated and interpreted, and the reportable

result to be calculated, without bias or manipulation of data. Staff should be encouraged to admit any mistakes and there must be a no-blame culture in place based on the leadership of senior management from the foundation level of the model. It is also important not to forget the importance of the overall pharmaceutical quality system in providing the umbrella for quality such as the investigation of out-of- specification results, managing deviations and developing corrective and preventative actions. **Figure 3** shows an analysis in practice and how the various levels of the data integrity model interact with each other. There are also the following elements of data governance:

- performing the work correctly and contemporaneously including any deviations
- effective and comprehensive second person reviews of the work
- visibility of errors
- investigation of aberrant results
- availability of both paper and electronic records for audit or inspection
- monitoring the development and maintenance of operational data integrity procedures and training.
- These complete the laboratory levels of the data integrity model shown in Figure 3 but don't forget the quality oversight (checks of current work plus data integrity audits and investigations) shown in Figure 1.

Quality Does Not Own Quality Anymore

Figure 3 shows how the various levels of the laboratory data integrity model interact together. However, without the Foundation layer, how can the three other layers hope to succeed? The onus is on trained staff to act ethically. Also, without qualified analytical instruments and validated software, how can you be assured of the quality and integrity of the data used to calculate the reportable result? And so on up the levels of the model. It is less important where an individual activity is placed in the various layers; the primary aim of this model is to visualize for chromatographers and analytical scientists the complete scope of data integrity.

If the data integrity model works from the foundation through the three levels that exist on top, it means that the responsibilities for data integrity and data quality are now dispersed throughout the laboratory and organization, whilst the overall accountability for quality oversight remains with a quality assurance function. It is not the role of quality assurance to fix other people's mistakes. The responsibility for data integrity and data quality in the chromatography laboratory lies is with the analytical staff performing the work, showing that quality (that is, the quality control department) does not own quality anymore. Everyone in the laboratory and the whole organization does.

Data Integrity Guidances and the Data Integrity Model

When the material in the data integrity guidance documents from MHRA, FDA, EMA, WHO and PIC/S (Refs) are compared with the model, there are several gaps and there is no mention of:

- analytical instrument qualification and fitness for intended use in comparison with a heavy emphasis on control of computerized systems, nor
- analytical procedures, including robust

"If the data integrity model works from the foundation through the three levels that exist on top, it means that the responsibilities for data integrity and data quality are now dispersed throughout the laboratory and organization."

method development and procedure validation.

All layers of the data integrity model are essential to ensure data integrity in a chromatography laboratory.

Summary

In this column, we have looked at a four-layer data integrity model to cover the whole scope of a data integrity program. The layers are interactive; ensuring data integrity depends on a foundation of data governance, qualified analytical instruments, and validated software with properly developed and validated robust analytical procedures. In the next article in this series, we will look at a way of identifying data integrity vulnerabilities in paper processes and computerized systems.

References

(1) ISO 17025-2017 General requirements for the competence of testing and calibration laboratories. 2017, International Standards Organization: Geneva.

(2) M.E. Newton and R.D. McDowall, *LCGC North Am.* **36**(5), 330–335 (2018).

(3) M.E. Newton and R.D. McDowall, *LCGC North Am.* **36**(1), 46–51 (2018).

(4) M.E. Newton and R.D. McDowall, *LCGC North Am.* **36(**4), 270–274 (2018).

(5) M.E. Newton and R.D. McDowall, *LCGC North Am.* **36**(7), 458–462 (2018).

(6) M.E. Newton and R.D.McDowall, *LCGC North Am.* **36**(8), 527–529 (2018).

(7) M.E. Newton and R.D. McDowall, *LCGC North Am.* **36**(9), 686–692 (2018).

(8) ICH Q10 Pharmaceutical Quality Systems. 2008, ICH, Geneva.

(9) EudraLex - Volume 4 Good Manufacturing Practice (GMP) Guidelines, Chapter 1 Pharmaceutical Quality System. 2013, European Commission: Brussels.

(10) Work plan for the GMP/GDP Inspectors Working Group for 2018 2017, European Medicines Agency: London.

(11) R.D. McDowall, *Data Integrity and Data Governance: Practical Implementation in Regulated Laboratories.* (Royal Society of Chemistry Publishing, Cambridge, UK, 2019).

(12) R.D. McDowall, *Validation of Chromatography Data Systems: Ensuring Data Integrity, Meeting Business and Regulatory Requirements* (Royal Society of Chemistry Publishing, Cambridge, UK, 2nd ed., 2017).

(13) R.D. McDowall, *Spectroscopy,* **31**(4), 15–25 (2016).

(14) G.P. Martin et al., Stumulus to the Revision Process: Proposed New USP General Chapter: The Analytical Procedure Lifecycle <1220> *Pharmacopoeial Forum*, **43**(1), 2017.

(15) M.E. Newton and R.D. McDowall, *LCGC Europe*, **30**(12), 679–685 (2017).

(16) EMA Questions and Answers: Good Manufacturing Practice: Data Integrity. 2016; Available from: http://www.ema.europa.eu/ema/index.

jsp?curl=pages/regulation/general/gmp_q_a.jsp&mid=WC0b01ac058006e06c#section9.

(17) MHRA GMP Data Integrity Definitions and Guidance for Industry 2nd Edition. 2015, Medicines and Healthcare products Regulatory Agency: London.

(18) MHRA GMP Data Integrity Definitions and Guidance for Industry 1st Edition. 2015, Medicines and Healthcare products Regulatory Agency: London.

(19) MHRA GXP Data Integrity Guidance and Definitions. 2018, Medicines and Healthcare products Regulatory Agency: London.

(20) WHO Technical Report Series No.996 Annex 5 Guidance on Good Data and Records Management Practices. 2016, World Health Organization: Geneva.

(21) PIC/S PI-041 Draft Good Practices for Data Management and Integrity in Regulated GMP / GDP Environments. 2016, Pharmaceutical Inspection Convention / Pharmaceutical Inspection Co-Operation Scheme: Geneva.

(22) R.D. McDowall, Spectroscopy 33(9), 18–22 (2018).

(23) ISPE Cultural Excellence Report. 2017, International Society of Pharmaceutical Engineering: Tampa, FL.

(24) GAMP Good Practice Guide: Data Integrity - Key Concepts. 2018, International Society for Pharmaceutical Engineering: Tampa, FL.

(25) FDA Guidance for Industry Out of Specification Results. 2006, Food and Drug Administration: Rockville, MD.

(26) USP 41 General Chapter <1058> Analytical Instrument Qualification. 2018, United States Pharmacopoeia Convention Rockville, MD.

(27) GAMP Good Practice Guide A Risk Based Approach to GXP Compliant Laboratory Computerised Systems, Second Edition 2012, Tampa, FL: International Society for Pharmaceutical Engineering.

(28) R.D. McDowall, Spectroscopy 32(9), 24–30 (2017)

(29) P.E. Smith and R.D. McDowall, *LCGC Europe* 31(7), 385–389 (2018).

(30) P.E. Smith and R.D. McDowall, *LCGC Europe* 31(9), 504–511 (2018).

(31) R.D. McDowall and C. Burgess, *LCGC North Am.* **33**(8), 554–557 (2015).

(32) R.D. McDowall and C. Burgess, *LCGC North Am.* **33**(10), 782–785 (2015).

(33) R.D. McDowall and C. Burgess, *LCGC North Am.* **33**(12), 914–917 (2015).

(34) R.D. McDowall and C. Burgess, *LCGC North Am.* **34**(2), 144–149 (2016).

(35) 21 CFR 211 Current Good Manufacturing Practice for Finished Pharmaceutical Products. 2008, Food and Drug Administration: Sliver Springs, MD.

(36) ICH Q2(R1) Validation of Analytical Procedures: Text and Methodology. 2005, International Conference on Harmonisation: Geneva.

(37) FDA Draft Guidance for Industry: Analytical Procedures and Methods Validation 2000, Food and Drug Administration: Rockville, MD.

(38) FDA Guidance for Industry: Analytical Procedures and Methods Validation for Drugs and Biologics. 2015, Food and Drug Administration Silver Springs, MD.

(39) G.P. Martin et al., *Pharmacopoeial Forum* **38**(1), 2012.

(40) Concept Paper: Analytical Procedure Development and Revision of ICH Q2(R1) Analytical Validation. 2018, International Council on Harmonisation: Geneva.

R.D. McDowall *is the director of RD McDowall Limited in the UK. Direct correspondence to: rdmcdowall@btconnect.com*

This article was originally published in LCGC North Amer. *37 (1), 44–51 (2019).*

Using Data Process Mapping to Identify Integrity Gaps

R.D. McDowall

Understanding and mitigating risks to regulatory records is an important part of a data integrity program. We discuss data process mapping as a technique to identify data gaps and record vulnerabilities in a chromatographic process and look at ways to mitigate or eliminate them.

Welcome to the second installment of "Data Integrity Focus." In the last part, we looked at the overall scope of a data integrity and data governance program via a four-layer model (1–3). In this part, we look at a simple and practical methodology that can be applied to identify the risks with any process in a regulated "good practice" (GXP) laboratory. Once identified, the risks can be mitigated or eliminated to ensure the integrity of data and records. The methodology is called data process mapping, and it is a variant of process mapping, which some of you may be familiar with if you have been involved with implementation of a computerized system or six sigma improvement project.

Once the process is mapped, the data and records created, modified, or calculated are identified and assessed to see if there any data vulnerabilities in a paper process or computerized system.

Ignore Paper Processes at Your Peril!

It is very important to understand that data integrity is not just a computer or information technology (IT) equipment problem. There are many manual process generating paper records that occur in the laboratory, such as sampling, sample preparation, calculation, and review (3–5). Many observation tests such as appearance, color, and odor are typically recorded on paper. Even with a computerized system, there are additional and essential paper records, such as the instrument and column log books.

What Do the Regulators Want?

What do the regulatory guidance documents say about assessment of processes? There are three documents that

I would like to focus on. The first is the World Health Organization (WHO) in their guidance document (6), that notes:

- 1.4. Mapping of data processes and application of modern quality risk management (QRM) and sound scientific principles throughout the data life cycle;
- 5.5. Record and data integrity risks should be assessed, mitigated, communicated, and reviewed throughout the data life cycle in accordance with the principles of QRM.

The second is the UK's Medicines and Healthcare products Regulatory Agency (MHRA) in their 2018 GXP guidance, which makes the following statements about assessment of processes and systems (7):

- 2.6 Users of this guidance need to understand their data processes (as a life cycle) to identify data with the greatest GXP impact. From that, the identification of the most effective and efficient risk-based control and review of the data can be determined and implemented.
- 3.4 Organizations are expected to implement, design, and operate a documented system that provides an acceptable state of control based on the data integrity risk with supporting rationale. An example of a suitable approach is to perform a data integrity risk assessment (DIRA) where the processes that produce data or where data are obtained are mapped out and each of the formats and their controls are identified, and the data criticality and inherent risks documented.
- 4.5 The data integrity risk assessment (or equivalent) should consider factors required to follow a process or perform a function. It is expected to consider not only a computerized system, but also the supporting people, guidance, training, and quality systems. Therefore, automation or the use of a "validated system" (such as analytical equipment) may lower but not eliminate data integrity risk.

The third and final guidance is from the Pharmaceutical Inspection Cooperation Scheme (PIC/S) (8):

- 5.2.2 Data governance system design, considering how data is generated, recorded, processed, retained and used, and risks or vulnerabilities are controlled effectively;
- 5.3.2 Manufacturers and analytical laboratories should 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.
- 5.3.4 Not all data or processing steps have the same importance to product quality and patient safety. Risk management should be utilized to determine the importance of each data or processing step. An effective risk management approach to data governance will consider data criticality (impact to decision making and product quality) and data risk (opportunity for data alteration and deletion, and likelihood of detection or visibility of changes by the manufacturer's routine review processes).

From this information, risk-proportionate control measures can be implemented.

Summarizing the guidance documents:

- Processes should be assessed to identify the data generated and the vulnerabilities

"Instead of starting with a fixed checklist, start with a blank whiteboard or sheet of paper together with some Post-it notes, pencils, and an eraser."

of these records, and this assessment should be documented.

- Vulnerabilities and risks to records must be mitigated or eliminated, and the extent of the controls used depends on the data criticality and risk to the records.
- In some cases systems should be replaced, and there should be a plan for this over a reasonable timeframe,
- Management must accept the process risk and support the migration plan.

Enter the Checklist

Typically, assessment of computerized systems involves a checklist where questions are posed for a spectrometer and the associated computerized system, such as:

- Does each user have a unique user identity?
- Is the audit trail turned on?
- Is there segregation of duties for system administration?

The checklist questions can go on, and on, and on, and, if you are (un)lucky, it can go into such excruciating detail that it becomes much cheaper and safer than a sleeping pill. There are three main problems with a checklist approach to system assessment:

- The checklists are not applicable to all computerized systems, as the questions may not cover all functions of the application
- Checklists can mislead an assessor into focusing too much on the checklist at the risk of not seeing additional data risks posed by a specific system
- Typically, checklists don't cover manual processes, of which there are many in a laboratory.

If a checklist is not the best tool, what tool should be used to identify data and records and then understand the risks posed?

Principles of Data Process Mapping

Instead of starting with a fixed checklist, start with a blank whiteboard or sheet of paper together with some Post-it notes, pencils, and an eraser. Why the eraser? You are not going to get this right the first time, and you'll be rubbing out lines and entries on the notes until you do. You'll need a facilitator who will run the meeting and two to three experts (perhaps laboratory administrators) who know the process, and, if software is involved, how the application works at a technical level.

The first stage is to visualize the process. Define the start and end of an analytical process (for example, from sampling to reportable result). The process experts should write the stages of the process down on the notes, and place them on the whiteboard or paper in order. The first attempt will be rough and will need revising,

as the experts can miss activities, or some activities will be in the wrong order, or the detail is uneven. The facilitator should encourage and challenge the experts to revise and refine the process flow, which may take two or three attempts. Although you can use a program like Visio to document the process, this slows the interaction between the participants during the initial mapping. I would suggest paper and pencil or whiteboard is an easier, and more flexible, option at this stage. When the process is agreed, then commit the final maps to software.

The second stage is to document data inputs, outputs, processing, verification steps, and storage for each of the process activities. This can involve manual data recording in log books, laboratory notebooks, and blank forms, as well as inputs to and outputs from any computerized systems involved in the process. Typically, such a process has not been designed, but has evolved over time, and can often look like a still from Custer's Last Stand with the number of arrows involved. This is the data process map or what we can call *the current way of working*.

Once the process is complete and agreed, look at each step and document:

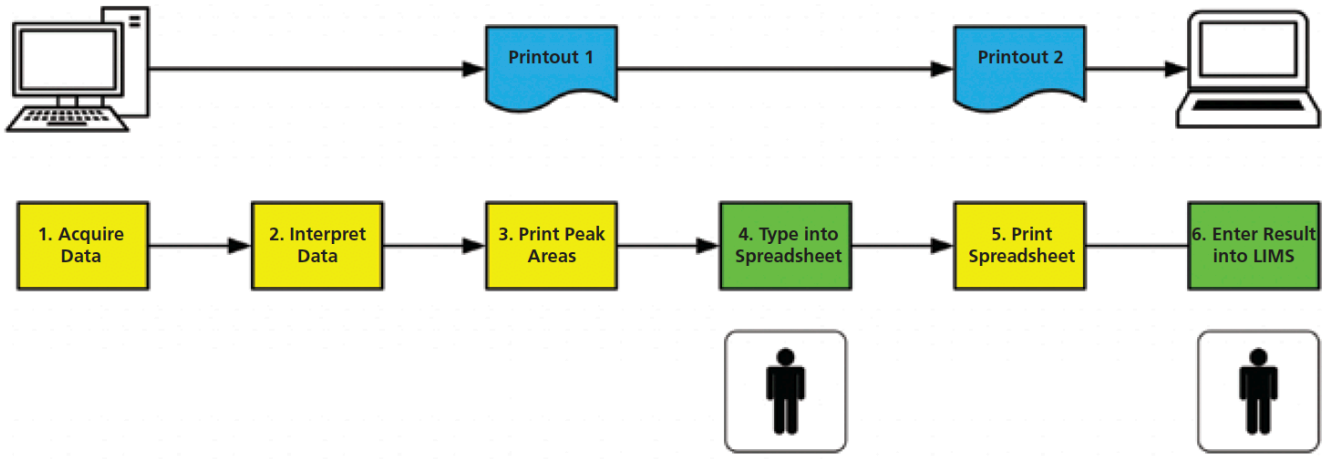
- How critical is each activity within the overall process (for example, product submission, release, stability, analytical development, and so on)?
- Where are the data and records stored in each activity?
- Are the data vulnerable at each stage?
- What is the reason for the vulnerability? (Reasons may include, but are not limited to, manual recording, or manual data transfer between a standalone instrument and another application)
- Are data entered into a computerized system manually, how is this checked, and how are corrections documented?
- Who can access the data? (Consider both paper and electronic records)
- Are the access controls for each application adequate, and are there any conflicts of interest?
- Are data corrections captured in an audit trail and, most importantly, are the entries understandable, transparent, and clear (9)?
- Are the responsibility for all steps and data clearly described, such as decisions or further actions taken and attributed to an individual?
- Is the data verification process clearly described, such as ensurance of accuracy of measurement, double checks performed (if any), and the review of the whole data package?

Any vulnerabilities need to be risk assessed, and remediation plans need to be developed. These plans will fall into two areas: quick fix remediation and long-term solutions. We will look at these two areas now for an example involving a chromatography data system.

Practical Example for Chromatography

From the theory, we need to look at how data process mapping could work in practice with a chromatograph linked to a chromatography data system (CDS). Welcome to a chromatography laboratory near to

Figure 1: Current hybrid process for chromatographic analysis.



you operating the world's most expensive electronic ruler, as shown in **Figure 1.**

Let me describe the main features of the simplified process:

- The chromatograph and CDS are set up for the analysis (we'll not consider the manual, paper-based sampling and sample preparation, because this was discussed recently by Newton and McDowall (4), together with the related data integrity problems).
- Although there are several instances of the same CDS, they are all standalone systems, and not networked together.
- There is a shared log on for all users, and this account has all privileges available, including the ability to configure the software.
- Paper printouts are considered the raw data from each instance of the CDS.
- Electronic records are backed up by the chromatographers when they have time, using a variety of media such as USB sticks and hard drives.
- Peaks are integrated, but there is no standard operating procedure (SOP) or control over the integration, such as when manual integration can or cannot be used (2,10).
- The integrated chromatograms are printed out.
- Peak areas from the printouts are entered manually into a spreadsheet (unvalidated, naturally!), to calculate system-suitability test (SST) parameters and the reportable results.
- The calculations are printed and signed, but the spreadsheet file is not saved.
- The results are entered manually from the spreadsheet printout into a laboratory information management system (LIMS) for release.
- The second-person review is not shown in this figure for simplicity, but this is a crucial part for ensuring data integrity (11).

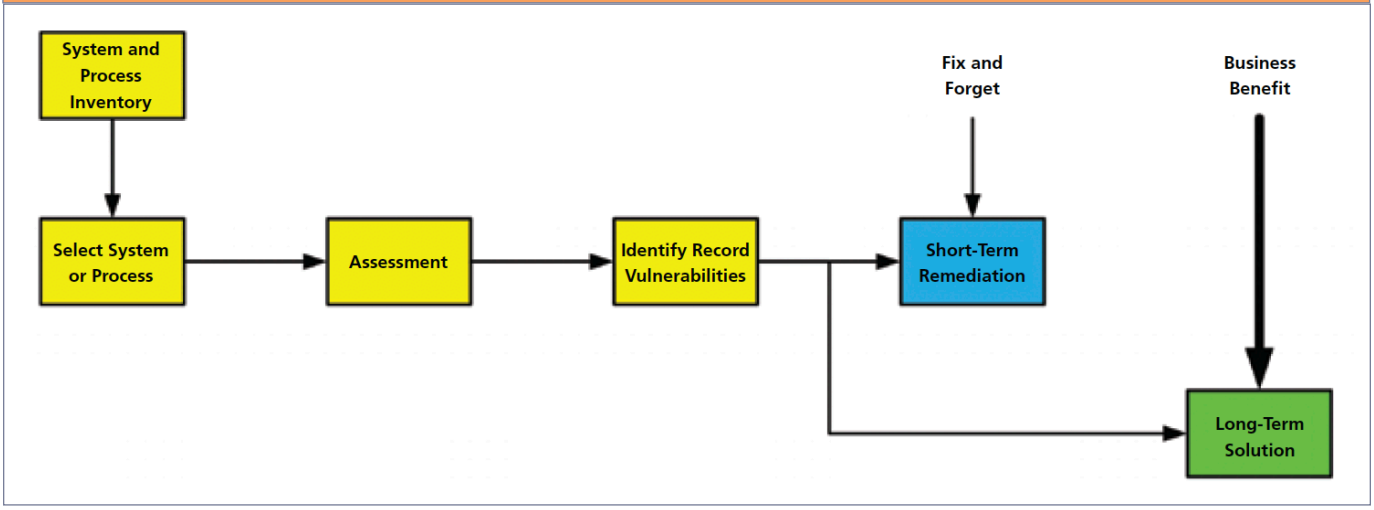
Some of you may be reading the process with abject horror, and may think

Table I: Main data vulnerabilities identified in a chromatography process

Process Step	Data – Record Vulnerability
1. Acquire Data	• No attribution of action: all users share one account • Conflict of interest: all users are administrators • Standalone system • Backup is performed by the lab users and is ad hoc • Ability for users to configure the CDS: turn functions on and off • Manual input of sample and sample preparation data, such as identity, lot number, sample weights, dilutions
2. Interpret Data	• No attribution of action: All users share one account • No standard operating procedure (SOP) for integration • No control of manual integration
3. Print Peak Areas	• Paper is considered the raw data by the laboratory • Risk of paper and e-records being different
4. Type into Spreadsheet	• Typographical errors when peak areas entered • No verification that calculations are correct as spreadsheet is unvalidated
5. Print Spreadsheet	• Failure to save the electronic spreadsheet file • No record signature linking to comply with Part 11 between paper printout and e-record • Must re-enter all data in a new spreadsheet if there is a typographical error
6. Enter Results into LIMS	• Typographical errors when results are entered • Secondpperson review only looks at paper records

that this would never occur in a 21st century chromatography laboratory. Based on my experience, and this is also seen in numerous U.S. Food and Drug Administration (FDA) warning letters, this process is more common than you may think. Remember that the pharmaceutical industry is ultraconservative, and if it worked for the previous inspection, all is well. However, to quote that world-famous chromatographer, Robert Zimmerman, the times, they are a-changin'. Hybrid systems (discussed in the next part of this series) are not encouraged by at least one regulator (6), and now some inspectors are unwilling to accept procedural controls to mitigate record vulnerabilities.

Figure 2: Remediate or solve data integrity vulnerabilities?



Identifying Record Vulnerabilities

Once the process is mapped, reviewed, and finalized, the data vulnerabilities can be identified for each process step. The main data vulnerabilities identified in the current chromatographic process steps are listed in Table I. To put it mildly, there are enough regulatory risks to generate a cohort of warning letters. There are many data integrity red flags in this table, including the fact that work cannot be attributed to an individual, defining raw data as paper, and failing to backup, or even save, electronic records. There is also the shambles of the business process, due to the use of the spreadsheet to calculate all the values from SST parameters and reportable results. Overall, the process is slow and inefficient. These risks need to be mitigated as an absolute minimum or, even better, eliminated entirely.

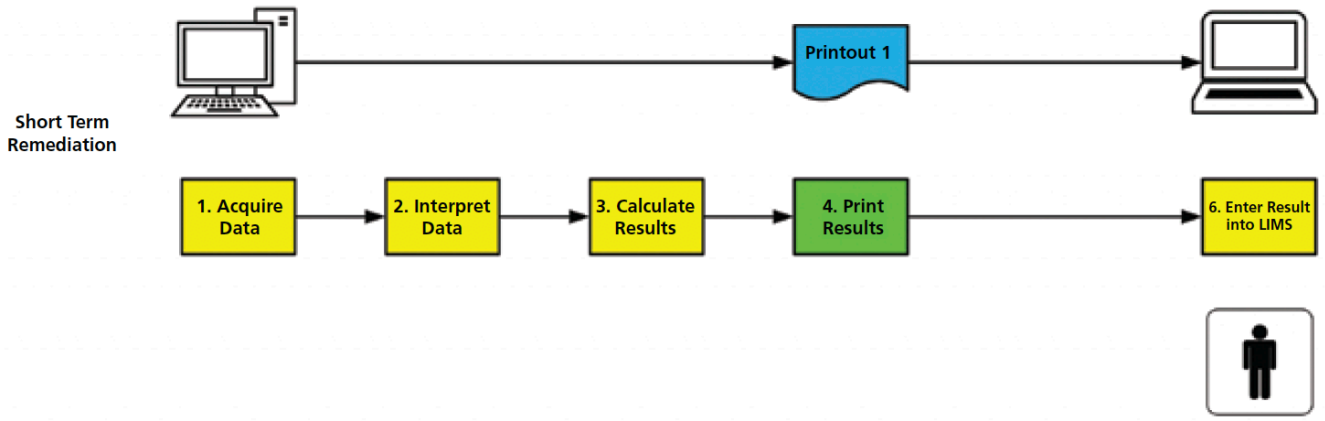
Fix and Forget or Long-Term Solution?

Enter stage left that intrepid group: senior management. These are the individuals who are responsible and accountable for the overall pharmaceutical quality system, including data integrity. The approaches that a laboratory will take are now dependent on them.

Figure 2 shows the overall approach that should happen to resolve data integrity issues. There are two outcomes:

1. Short-term remediation to resolve some issues quickly. Ideally, this should involve technical controls where available (for example, giving each user a unique user identity, or creating and allocating user roles for the system and segregation of duties). However, remediation often involves procedural controls, such as the use of SOPs or log books to docu-

Figure 3: Short term remediation of the chromatography process.



ment work. This slows the process down even further, and will result in longer second-person review times (11).

2. Long-term solutions to implement and validate technical controls, to ensure that work is performed correctly and consistently. This should involve replacement of hybrid systems with electronic working and ensuring business benefit from the investment in time and resources.

The problem is management. In many organizations, they want only to focus on the first option (fix and forget) and not consider the second, as it would detract from the work or cost money. While this may be thought to be an option in the very short term, it is not viable when regulatory authorities become more focused on hybrid systems with procedural controls.

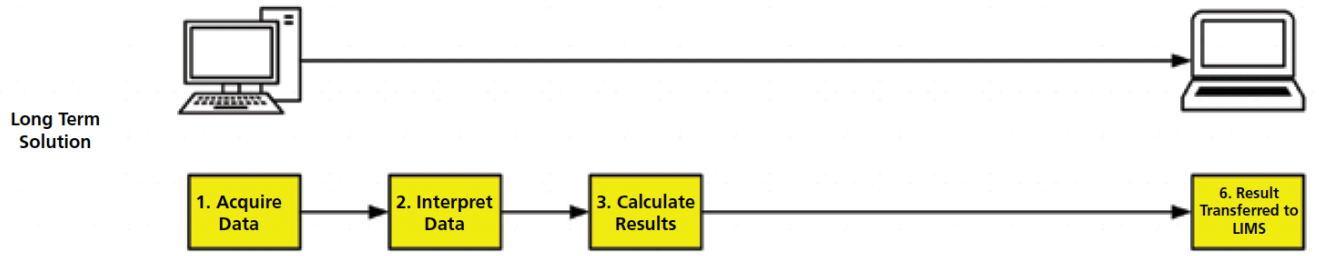
In organizations that claim there is no money to provide long-term solutions, however, the financial taps are quickly turned on following an adverse regulatory inspection. However, it is better, more efficient, and cheaper to implement the long-term solution yourself, because then the company, not the regulator, is providing the solution.

Quick Fixes and Short-Term Remediation

From the data process map in Figure 1, some short-term solutions can be implemented as shown in **Figure 3.** Rather than attempt to fix a broken and inefficient process, use the CDS software that the laboratory has paid for to calculate the SST and final results. This would eliminate the spreadsheet, as well as manual entry into the spreadsheet and subsequent transcription checks.

Attention must also be focused on the CDS application, and some of the main changes for immediate implementation must be:

Figure 4: Long-term solution for the chromatographic process.



- Unique identities for all users
- Implement user types with access privileges, and allocate the most appropriate one to each user
- Segregation of application administration from normal laboratory users is more difficult, as the systems are currently standalone, and will probably require a two-phase approach: Short-term with laboratory administrators having two access types, one with administration functions (user account management and application configuration) but no access to CDS functions, and vice versa. This approach should only be used as a temporary fix, and not a permanent solution.
- Write an SOP for chromatographic integration, and specifically control when manual integration can be used (2,10,12), and train the staff. Where feasible, restrict a user's ability to perform manual integration for some methods.
- Validate and use the CDS application ability to calculate SST parameters and eliminate the spreadsheet calculation (the former should be relatively easy to implement). Calculation of the reportable result may have to wait until the CDS is networked. In the latter case, the spreadsheet calculations will need to be validated and all files saved.

This should result in an improved business process, as shown in Figure 3. The CDS is still a hybrid system, but the spreadsheet has been eliminated, along with manual entry to a second system, but the process is under a degree of control. Left like this (the fix and forget option from Figure 2), there is substantial risk remaining in the process, such as backup of the standalone systems and the need for plans for a long-term solution.

Implementing Long-Term Solutions

Long-term solutions require planning, time, and money. However, with the potential business and regulatory benefits that can be obtained, management should be queuing up to hand over money. Let us look at some of the remaining issues to try and solve with this process:

- Standalone CDS systems need to be implemented into a networked solution including the migration of existing data

to the central server. This has several advantages: IT backup of records, IT application administration, and time and date stamps from the network time server.
- Consistency of operation: The same methods can be applied across all chromatographs.
- Removal of a hybrid system: Design the networked CDS for electronic working and electronic data transfer to the LIMS, which results in minimal or zero paper to be printed out.
- Efficient, effective, and faster business process, as shown in **Figure 4,** and this should be compared with that in Figure 1.

The regulatory risks of the original process have been greatly reduced or eliminated at the end of the long-term solution. The laboratory can face regulatory inspections with confidence.

Acknowledgement

I would like to thank Christine Mladek for helpful review comments during preparation of this column.

References

1 R.D. McDowall, LCGC North Amer. 37(1), 44–51 (2019).

2 R.D McDowall, Validation of Chromatography Data Systems: Ensuring Data Integrity, Meeting Business and Regulatory Requirements (Royal Society of Chemistry, Cambridge, UK, 2nd Ed., 2017).

3 R.D. McDowall, Data Integrity and Data Governance: Practical Implementation in Regulated Laboratories (Royal Society of Chemistry, Cambridge, UK, 2019).

4 M.E. Newton and R.D. McDowall, LCGC North Amer. 36(1), 46–51 (2018).

5 M.E. Newton and R.D. McDowall, LCGC North Amer. 36(4), 270-274 (2018).

6 WHO Technical Report Series No. 996 Annex 5 Guidance on Good Data and Records Management Practices. 2016, World Health Organization: Geneva.

7 MHRA GXP Data Integrity Guidance and Definitions. 2018, Medicines and Healthcare products Regulatory Agency: London.

8 PIC/S PI-041 Draft Good Practices for Data Management and Integrity in Regulated GMP / GDP Environments. 2016, Pharnaceutical Inspection Convention / Pharmaceutical Inspection Co-Operation Scheme: Geneva.

9 R.D. McDowall, Spectroscopy 32(11), 24-27 (2017).

10 Technical Report 80: Data Integrity Management System for Pharmaceutical Laboratories. 2018, Parenteral Drug Association (PDA): Bethesda, MD.

11 M.E. Newton and R.D. McDowall, LCGC North Amer. 36(8), 527–529 (2018).

12 M.E. Newton and R.D. McDowall, LCGC North Amer. 36(7), 458–462 (2018).

R.D. McDowall *is the director of RD McDowall Limited in the UK. Direct correspondence to: rdmcdowall@btconnect.com*

This article was originally published in LCGC North Amer. *37 (2), 44–51 (2019).*

What Is the Problem with Hybrid Systems?

R.D. McDowall

Regulatory authorities globally have concerns about hybrid computerized systems. These are the worst possible computerized system to have in your laboratory from a regulatory perspective. Here, we discuss what a hybrid system is, and explain why there is such a fuss about them.

This article is the third in a six-part series dealing with data integrity. The first discussed a data integrity model to present the scope of data integrity and data governance program for an organization (1). The second discussed data process mapping to identify data integrity gaps in a process involving a chromatography data system (CDS), and looked at ways to remediate these gaps (2). The CDS was described originally as a hybrid system, and I mentioned that this subject would be the topic of this third article.

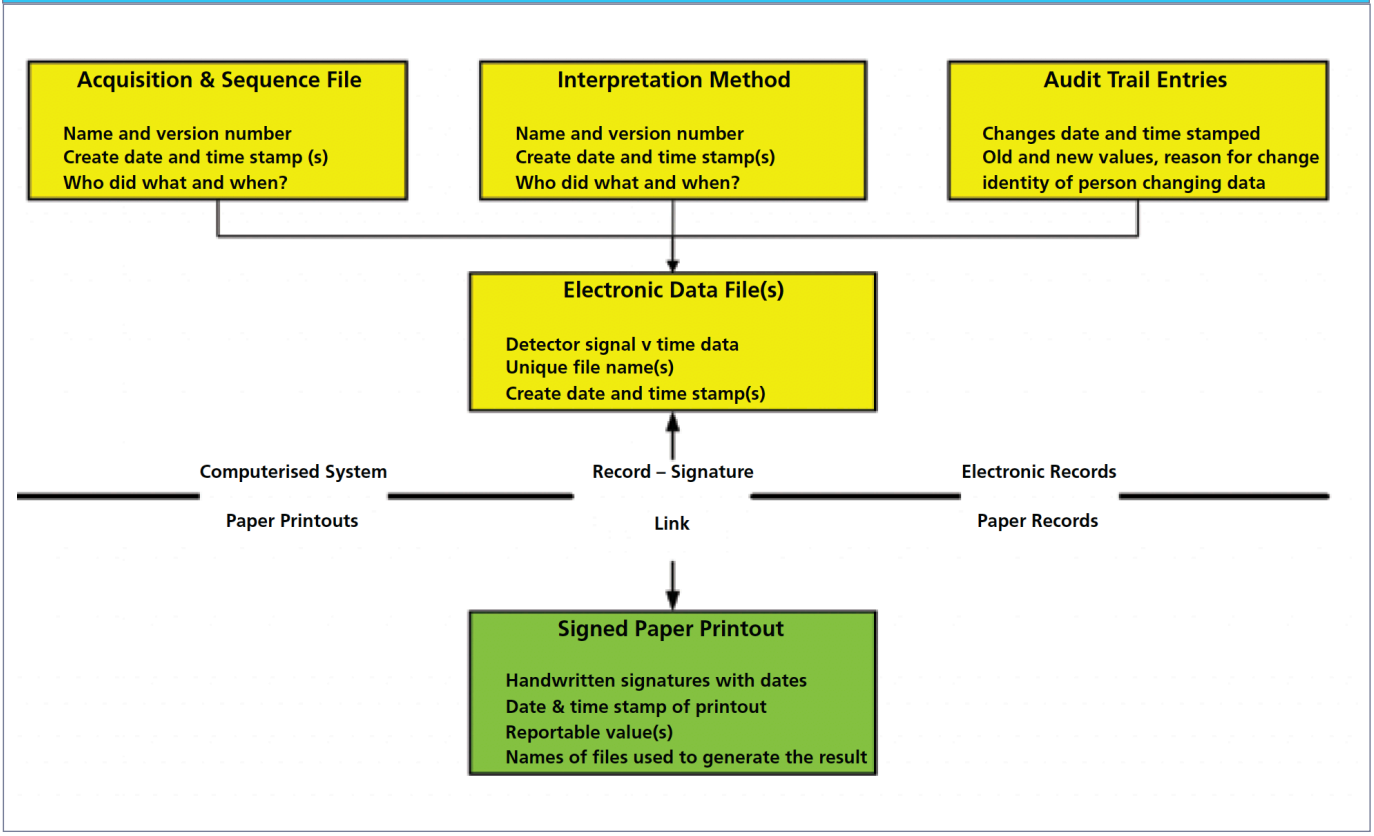
What is a Hybrid System?

First, it is important to define what we mean by a *hybrid computerized system*. The best definition and description is found in the World Health Organization (WHO) guidance (3):

> *This refers to the use of a computerized system in which there is a combination of original electronic records and paper records that comprise the total record set that should be reviewed and retained.*
>
> *An example of a hybrid approach is where laboratory analysts use computerized instrument systems that create original electronic records and then print a summary of the results.*
>
> *The hybrid approach requires a secure link between all record types, including paper and electronic, throughout the records retention period.*
>
> *Where hybrid approaches are used, appropriate controls for electronic documents, such as templates, forms and master documents, that may be printed, should be available.*

A schematic of a hybrid computerized system is shown in **Figure 1.** There are a

Figure 1: A schematic of a hybrid system consisting of electronic records and signed paper printouts (4).



number of electronic records within the computerized system, and these must be securely linked with the paper printouts that are signed by the analyst and reviewer. Often, the focus is only on the paper printout and not the electronic records when, in fact, it should be the other way around; e-records are the critical data, and signed paper printouts are only a small part of the records.

Unable Able Laboratories

Able Laboratories is the classic data integrity case study that can be summarized as "You can't falsify data into compliance." This now defunct generic pharmaceutical company had passed several US Food and Drug Administration (FDA) inspections before a whistleblower called to alert the agency about fraudulent quality control (QC) work. Inspectors quickly found that data were being falsified on an industrial scale, using a variety of means such as copy and paste, manipulation of weights, and chromatographic integration (5). The heart of the falsification effort was a CDS in which the audit trail that could not be turned off identified who had falsified which data and when. The reason why the agency had missed the falsification is that the inspectors focused on paper printouts alone. As a result, there were changes to

the way FDA and other regulatory agencies inspect computerized systems with updated regulations (6,7) and guidance (3, 8–11), as we will discuss now.

What the Regulators Want

In addition to providing a definition of *hybrid system*, the WHO good records management practices guidance also notes, in Appendix 1, under special risk factors in the Attributable section (3):

The use of hybrid systems is discouraged, but where legacy systems are awaiting replacement, mitigating controls should be in place.

> *In such cases, original records generated during the course of [good practice] GXP activities must be complete and must be maintained throughout the records retention period in a manner that allows the full reconstruction of the GXP activities.*
>
> *A hybrid approach might exceptionally be used to sign electronic records when the system lacks features for electronic signatures, provided adequate security can be maintained. The hybrid approach is likely to be more burdensome than a fully-electronic approach; therefore, utilizing electronic signatures, whenever available, is recommended.*
>
> *Replacement of hybrid systems should be a priority.*

Have you got the message? Hybrid systems are not liked, and using them to ensure data integrity will cost you time and effort. The WHO guidance goes about as far as a regulatory guidance can go by stating that hybrid systems are discouraged, and that they should be replaced as a matter of priority. The Pharmaceutical Inspection Co-operation Scheme (PIC/S) PI-041 Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments also notes in section 9.3 (10):

> *Increased data review is likely to be required for hybrid systems.*

This is true as a second person reviewing hybrid records must review both paper and electronic records plus the linkages between the two types of records as shown in Figure 1, making the review more labor intensive and slow. As Newton and McDowall noted, the second person review may take longer than the actual chromatographic run (12).

The World Consists of Hybrid Systems

OK, saying that the world consists of hybrid systems is not quite accurate, but, in many laboratories, standalone hybrid computerized systems are used. Even networked systems with the technical controls to be used electronically can be deployed in hybrid mode, because this approach is seen as a tried and trusted option. This viewpoint is wrong, and dangerously so.

There are now more stringent controls placed on hybrid systems, especially if it is a standalone workstation. Regulatory guidance notes that hybrid systems will probably result in more review work compared

with an electronic process, and at the same time regulatory exposure will increase over time as interpretation becomes tighter. By failing to replace hybrid systems, management must accept accountability for its inaction when an inspector calls and finds a data integrity problem. To understand the situation from the perspective of the regulations, we need to go back in time to the last century.

Understanding the "c" in cGMP

Have you ever wondered why the FDA Good Manufacturing Practice (GMP) regulations have the word *current* in the title? To find out why we need to go back in time to September 29, 1978, and the publication of FDA's *Current Good Manufacturing Practice* (cGMP) regulations in the *Federal Register* (13). You may ask why we should bother with something that was published in the mists of time, when all we need to do is an Internet search as find the GMP regulations on the web. Not quite, dear reader. If you bother to read the regulations you will find that there is no definition or explanation of the word *current* in the regulation (for the purists, there is also no mention of *current* in the definitions of cGMP in 21 *CFR* 210).

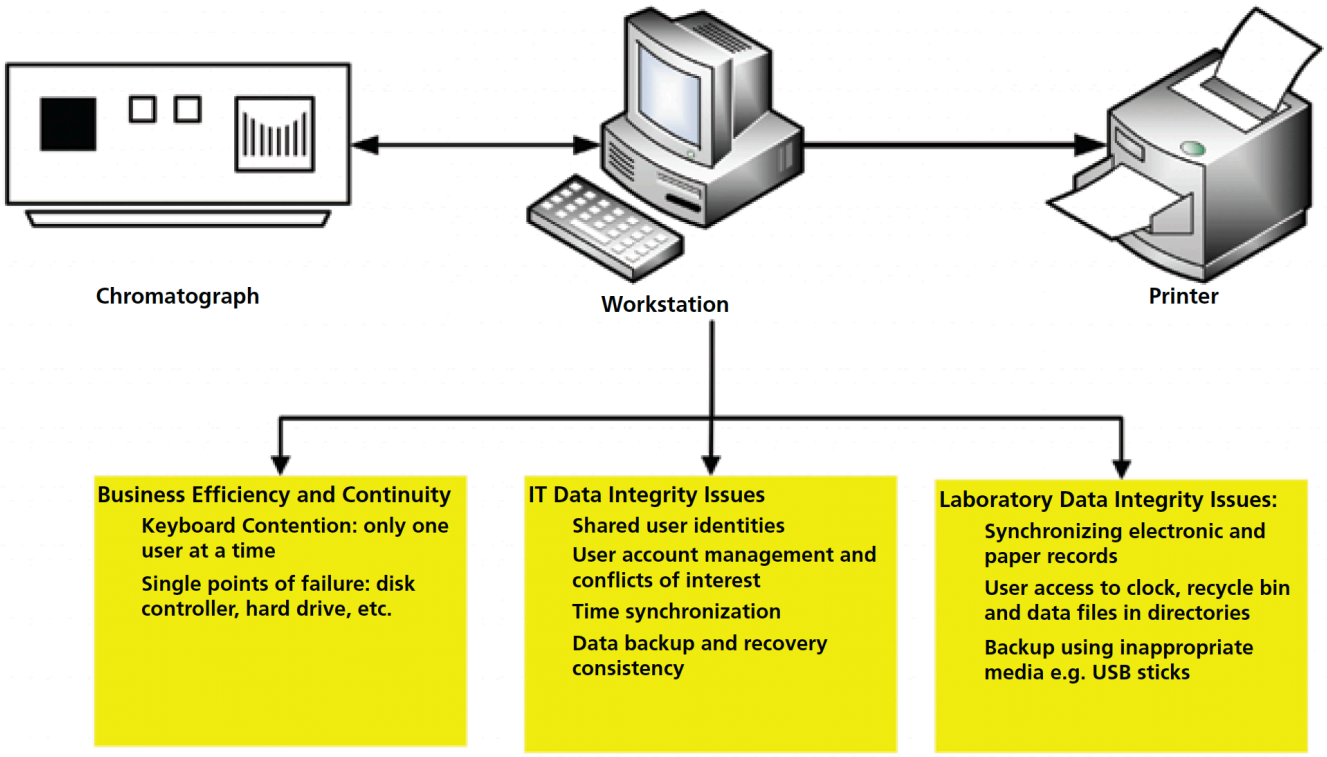
The way that current was intended to be used will be found in preamble comment 17 of the regulations published in 1978 (13). It is built into the GMP regulation from the beginning, and not slipped in as an afterthought. In the scope section of the regulation (21 *CFR* 211.1), it states that:

(a) The regulations in this part contain the minimum current good manufacturing practice for preparation of drug products for administration to humans or animals.

The 21 *CFR* 211 regulations are stated to be the minimum expected. The problem with the pharmaceutical industry is that these regulations are typically interpreted as "These directives are all we will do." This divergence from the intent of the regulation is the start of some data integrity problems. We can delve further into an understanding of current in comment 17 of the 1978 preamble to the GMP regulations (13); here is a discussion on the use and meaning of the word current is as follows:

> *One comment recommended that the word "current" be deleted since it is obvious that the latest regulations to be published are current, and therefore the use of the word "current" is superfluous....*
>
> *Several of these comments reflect, the Commissioner believes, a misunderstanding regarding the use of the word "current"....*
>
> *The Congress intended that the phrase itself have a unique meaning and that the good manufacturing practice regulations represent sound current methods, facilities and controls for the production of drugs to assure safety…*
>
> *Although the practices must be "current" in the industry, they need not be widely prevalent. Congress did not require that a majority or any percentage of manufacturers already be following the proposed mandated practices, as long as it was a current good manufacturing practice in the*

Figure 2: Typical configuration of a hybrid chromatography data system and potential data integrity problems (4).



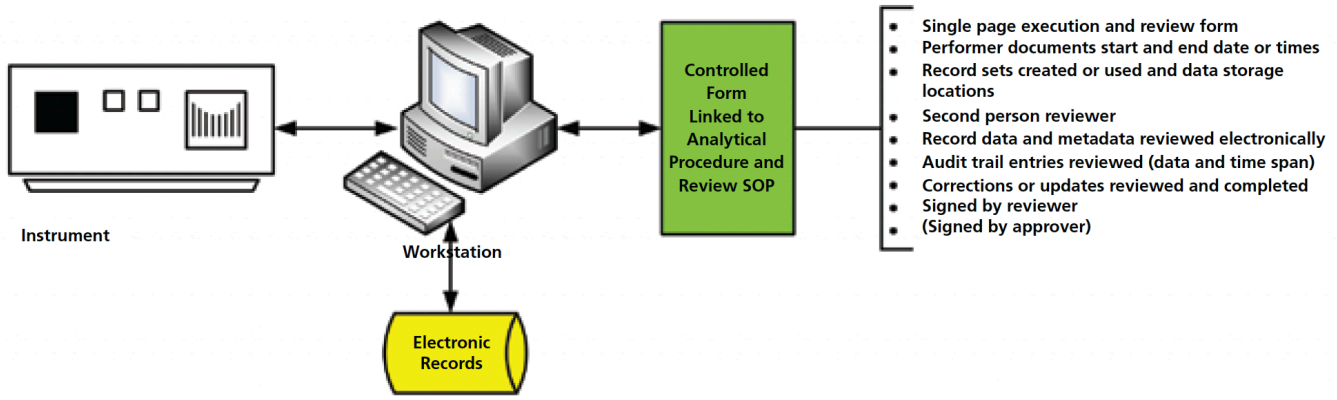
industry, i.e. that it had been shown to be both feasible and valuable in assuring drug quality (13).

The intent of the US GMP regulations has been that as science, analytical instrumentation, and technologies advance, then so too must the pharmaceutical industry. Even if an advance is not widely used in the industry, if it can ensure an improvement in drug quality, then it comes under the purview of the "c" in cGMP.

However, the problem is that reality in regulated laboratories does not match regulatory intent. Once a pharmaceutical organization has developed an interpretation of the regulation, it is reluctant to change for several reasons, such as the cost of new technology, validation costs, the cost of updating a registration dossier, and perceived or actual inflexibility of the inspectorate to accept such advances. The companies often prefer to remain with older processes that do not reflect the most effective and efficient ways of working, if they have not had any problems in the past.

Personal computers have been used for controlling chromatographs since the 1980s, and they have typically been designed to be used in the same way, as a hybrid system. Publication of 21 *CFR* 11 regulations (14) in 1997 allowed the use of electronic signatures, but widespread

Figure 3: A schematic of the generation and review of hybrid records (4).



adoption has not occurred. Large pharmaceutical companies have implemented site or global CDS with electronic signatures, but smaller companies typically have not gone in the same direction, preferring to have standalone systems, often from several different suppliers, which can be argued as crass stupidity.

Hybrid System Configuration and Data Integrity Issues

A typical hybrid system is shown in **Figure 2** and consists of three components:

- Analytical instrument, such as a chromatograph
- Controlling workstation, where the CDS software is loaded and where data are stored
- Printer

Figure 2 shows the potential data integrity problems that fall into three categories: business efficiency and continuity, IT data integrity, and laboratory data integrity. One of the major problems with hybrid systems is protecting the data and associated metadata with effective backup and recovery processes. If backup is left to the laboratory, it will inevitably fail, because backup is not the main function of a chromatography laboratory.

Are You Lazy?

Most hybrid systems print paper as if it is going out of fashion. Depending on the sadists in the Quality Assurance (QA) department, often each page must be initialled by the tester, and again by the reviewer, which is an error prone, tedious, and non-value-added task. The printouts must also be checked against the electronic records that were created or used in the analysis.

A simple way to reduce the amount of paper printed from a hybrid system is outlined in Appendix 1 of the WHO data integrity guidance (3). Shown in **Figure 3** is a controlled and uniquely numbered review form (10,15) for the creation and review of the records created during an analysis using a hybrid system. The form is linked to

the analytical procedure and standard operating procedure (SOP) for review of laboratory records. The steps are as described below.

- At the start of the analysis, a uniquely numbered version of the form is issued to the tester, who documents the start and end date and time of the analysis (to help the second-person reviewer search audit trail entries), as well as documents the records created, modified, and the location where they are stored.
- Chromatograms and data are reviewed by the analyst on screen. The only printout from the CDS is the test summary of the reportable results and analysis information.
- The results printout and review form is signed by the tester.
- When records are ready for review, a second analyst reviews files electronically on screen with no printouts; this makes the task simpler and quicker.
- The reviewer checks the data files and contextual metadata files generated by the performer of the test, and documents these on the review form. The applicable audit trail entries are also reviewed between the analysis start and end times and dates, and documented.
- Checks for falsification of data are included in the form, as this will be reviewed during data integrity audits and, if applicable, data integrity investigations.
- If changes are required to be made, these are documented and sent back to the tester to update. When the review is complete, the reviewer then signs the form. If required by laboratory procedures, there may be space on the form for an approval or QA signature.

This approach reduces the volume of paper printed, but also allows a faster review, as the cross check between the electronic and paper is far smaller than now.

"Working with hybrid systems–computerized systems that generate electronic records with signed paper printouts–is the worst possible world to be in."

Eliminate Hybrid Systems

Working with hybrid systems–computerized systems that generate electronic records with signed paper printouts–is the worst possible world to be in. The laboratory must manage two incompatible media formats: paper and electronic records. The best advice is to eliminate these systems by using electronic systems to ensure both regulatory compliance and business efficiencies, as we discussed in the second part of this series (2).

Why Are You Still Buying Hybrid Systems?

I could have entitled this subheading "Why are suppliers still selling hybrid systems?" However, given that suppliers respond to market forces, it is the responsibility of customers to put pressure on suppliers to design adequate systems for today's data integrity world. Laboratories that have assessed and remediated current systems are perpetuating the problem when new systems are purchased, because they are typically:

- standalone
- hybrid
- involve data being stored in directories created in the operating system rather than in a database

For further discussion regarding CDSs, please refer to the four-part series written for *LCGC North America* by Chris Burgess and myself (16–19).

The Year-End Slush Fund Spend?

You know the situation: A month before the end of the financial year, your boss puts his or her head round the door of the laboratory and says nonchalantly, "We have money to spend before the year end. Any ideas?" This question initiates a mad panic, because three quotes have to be generated, the capital request raised and walked around for signature, the purchase order raised, and an empty box delivered to stores. What a quality way to purchase instrumentation and software. It is extremely unlikely that the overall system has been adequately assessed for compliant functions and technical controls for data integrity. The staff only focus on the bright shiny instrument. However, this reaction perpetuates the data integrity problem. But this problem always occurs in other organizations, doesn't it?

> "The biggest problem with hybrid systems is the synchronization of two incompatible media."

Summary

We have defined what a hybrid system is, and why it is not recommended by regulatory authorities. The biggest problem with hybrid systems is the synchronization of two incompatible media. However, the hybrid problem is perpetuated by dumb suppliers who do not design software for electronic working and data acquisition directly to a network storage area. The problem is compounded by stupid laboratories that keep purchasing applications with inadequately designed compliance functions to give data integrity assessors a job for life.

References

1. R.D. McDowall, LCGC North Am. 37(1), 44–51 (2019).
2. R.D. McDowall, LCGC North Am. 37(2), 118–123 (2019).
3. WHO Technical Report Series No. 996 Annex 5 Guid-

ance on Good Data and Records Management Practices. World Health Organization, Geneva, Switzerland (2016).

4. R.D. McDowall, Data Integrity and Data Governance: Practical Implementation in Regulated Laboratories (Royal Society of Chemistry, Cambridge, UK, 2019).

5. Able Laboratories Form 483 Observations, 6 July 2005; Available from: http://www.fda.gov/downloads/aboutfda/centersoffices/officeofglobalregulatoryoperationsandpolicy/ora/oraelectronicreadingroom/ucm061818.pdf.

6. European Commission Health and Consumers Directorate-General, EudraLex: Volume 4 Good Manufacturing Practice (GMP) Guidelines, Chapter 4 Documentation, E. Commission, Ed. (Brussels, Belgium, 2011).

7. European Commission Health and Consumers Directorate-General, EudraLex: Volume 4 Good Manufacturing Practice (GMP) Guidelines, Annex 11 Computerized Systems, European Commission (Brussels, Belgium, 2011)

8. MHRA GMP Data Integrity Definitions and Guidance for Industry 2nd Edition. Medicines and Healthcare Products Regulatory Agency, London, UK (2015).

9. MHRA GXP Data Integrity Guidance and Definitions. Medicines and Healthcare Products Regulatory Agency, London, UK (2018).

10. PIC/S PI-041 Draft Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, Pharmaceutical Inspection Convention/Pharmaceutical Inspection Co-Operation Scheme, Geneva, Switzerland (2018).

11. EMA Questions and Answers: Good Manufacturing Practice: Data Integrity. 2016; Available from: http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/general/gmp_q_a.jsp&mid=WC0b01ac058006e06c#section9.

12. M.E. Newton and R.D. McDowall, LCGC North Am. 36(8), 527–529 (2018).

13. Current Good Manufacturing Practice for Finished Pharmaceuticals, in Code of Federal Regulations Title 21 Part 211, 43(190), 45014–45089 (U.S. Government Printing Office, Washington, DC, USA, 1978).

14. Food and Drug Administration, 21 CFR 11 Electronic Records; Electronic Signatures, Final Rule (FDA, Washington, DC, USA, 1997).

15. FDA Guidance for Industry Data Integrity and Compliance With Drug CGMP Questions and Answers (Food and Drug Administration, Silver Springs, MD, 2018).

16. R.D. McDowall and C. Burgess, LCGC North Am. 33(8), 554–557 (2015).

17. R.D. McDowall and C. Burgess, LCGC North Am. 33(10), 782–785 (2015).

18. R.D. McDowall and C. Burgess, LCGC North Am. 33(12), 914–917 (2015).

19. R.D. McDowall and C. Burgess, LCGC North Am. 34(2), 144–149 (2016).

R.D. McDowall *is the director of RD McDowall Limited in the UK. Direct correspondence to: rdmcdowall@btconnect.com*

Agilent CrossLab
From Insight to Outcome

Move Your Analytical Instrument Qualification to Agilent

At a time when laboratories are focusing on reducing costs, increasing productivity and maximizing return on investment, they need to be ready to address fundamental questions about the compliance of their Analytical Instrument Qualification (AIQ) during laboratory audits and inspections.

The Agilent Automated Compliance Engine is designed to simplify compliance with data integrity requirements, while providing a harmonized and cost-effective approach which is not limited to a particular instrument manufacturer or software.

Move to Agilent today! Visit www.agilent.com/chem/qualification

Agilent