# Data Integrity in Regulated and Accredited Environments
# Part 1: Fundamentals and Principles

**Dr David Trew BSc(Hons), PhD, CChem MRSC**

## 1 Introduction

It is a fundamental expectation and requirement that all scientific data and records are both reliable and trustworthy. When the data are used to make decisions concerning the health and safety of individuals, the quality of the environment, to support national and international trade, the detection of crime and the prosecution of offenders, the reliability and trustworthiness of those records is of critical importance.

In the heavily regulated pharmaceutical and healthcare sector, the integrity of manufacturing records and laboratory quality control testing continues to attract considerable regulatory scrutiny. The issue of unreliable manufacturing and testing records in the pharmaceutical industry was first identified in 2005 when US generic drug manufacturer Abel Laboratories was found by the US Food and Drug Administration (FDA) to have routinely resampled, re-injected or reprocessed samples of drug products during quality control testing when out of specification (OOS) results were obtained. Able Laboratories failed to report any of these OOS results, which were replaced by results conforming to specification.

Able Laboratories was forced to suspend production of, and recall all of its products from the market. With no production and no products, it was able to sell, the company's value fell by over 85 %, and by the end of 2005 the company had sold its assets to Sun Pharmaceuticals.

Since the Able Laboratories scandal the integrity of manufacturing records and laboratory testing data has continued to attract increasing scrutiny from the regulatory authorities and other stakeholders in the pharmaceuticals and life sciences sectors. More recently, Indian generic drug manufacturer Ranbaxy entered in to a consent decree with the FDA in January 2012.

The regulated pharmaceutical and life sciences sectors are not the only industries to experience scandals over fabricated records and data. For example, the accredited forensic analysis sector has been rocked by misconduct. In 2012 confidence in the entire Massachusetts judicial system was compromised when Annie Dookham, an analytical chemist working in the Massachusetts Forensic Drug Laboratory, analysing samples of seized drugs in criminal court cases, was discovered to have falsified the test results in samples for up to 40000 criminal drugs cases over a ten-year period. On 22 November 2013 Mrs. Dookham was convicted of falsifying evidence and was sentenced to 3 to 5 years in prison

# Data Integrity in Regulated and Accredited Environments Part 1: Fundamentals and Principles

Some of the regulatory authorities have published guidelines which elucidate their current thinking and expectations regarding the systems companies should have in place. These systems should be able to provide a high level of confidence that the data and records being used to make decisions concerning the quality of regulated products are reliable and trustworthy.

The United Kingdom Medicines and Healthcare Regulatory Authority published guidelines titled "MHRA GMP Data Integrity Definitions and Guidance for Industry"[1] in March 2015, and issued an undated version[2] as a consultation document in July 2016. In September 2015 the World Health Organisation published a draft "Guidance on Good Data and Record Management Practices"[3]. In addition, in April 2016 the FDA published a draft Guidance for Industry titled "Data Integrity and Compliance with CGMP"[4]. All of these guidelines advocate accurate, legible, contemporaneous, original and attributable, as fundamental requirements for achieving comprehensive data integrity. The Pharmaceutical Inspection Cooperation Scheme has also published a draft document "Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments"[5].

In addition to the guidance documents published by the regulatory agencies a number of articles have also been published addressing different topics. In the first part of a two-part article discussing the FDAs focus on laboratory data integrity, McDowall[6] identifies the following barriers to comprehensive data integrity:

- *Human errors when incorrect data is entered by mistake (an uncorrected fat finger moment), stupidity (not being aware of regulatory requirements or poor training) or wilfully (falsification or fraud with the intent to deceive)*
- *Selection of good or passing results to the exclusion of those that are poor or failing*
- *Unauthorized changes to data made post-acquisition*
- *Errors that occur when data is transmitted from one computer to another*
- *Changes to data through software bugs or malware of which the user is not aware*
- *Hardware malfunctions, such as disk crashes*
- *Changes in technology, where one item is replaced when it becomes obsolete or no longer supported, making old records unreadable or inaccessible*

This paper also discusses potential data integrity issues associated with chromatographic data systems (CDS) and discusses the deficiencies found during an inspection at Indian drug manufacturer RPS Life Sciences[7]. It is noted that all FDA inspectors have received training in data integrity. Also instead of looking at paper printouts, inspectors now look at the electronic records created by the CDS, and will request to be taken through the analysis and audit trails. It is also important to understand that it is the electronic records that are considered to be the data, not the paper printouts.

The second part of this article[8] discusses the Consent Decree[9] between Ranbaxy Laboratories and the US Food and Drugs Administration. The principle elements of this Consent Decree are:

- A requirement to establish an Office of Data Reliability in the US that is responsible for conducting audits of submissions to ensure integrity of data, including that from Quality Control.

- The Data Reliability Office must be headed by a Chief Data Reliability Officer (CDRO) who reports to the Managing Director (MD) of Ranbaxy Laboratories.
- One of the principle responsibilities of the CDRO is to recommend to the MD that specific staff members be disciplined or terminated for data manipulation, or that regulatory submissions should be withdrawn due to falsification of data.
- All existing drug applications are to be reviewed by a Data Integrity Expert to identify any falsified data.
- The audit trails need to be reviewed by the CDRO to identify data irregularities and whether these impact the integrity of the application.
- To establish a global toll-free number, publicized by the company to all employees, to allow staff members to raise concerns anonymously about working policies and practices that are non-compliant. This is intended to allow staff in the Data Reliability Office to pursue issues to determine if they are true or not and identify individuals who promoted the falsification activities.
- In addition, the company must engage an independent GMP auditor for five years to conduct compliance audits at specified Ranbaxy sites, reports from these audits are to be submitted to Ranbaxy management and the FDA.

In addition, Ranbaxy also paid a record breaking $500 million fine. This clearly demonstrates that complying with the regulations is a much more cost effective strategy than taking short cuts or seeking to conceal test results that do not show your products conform to specifications, and then having to cover the costs associated with remediation.

In an earlier article[10] published in 2011 McDowall suggests the following ten areas are essential for ensuring the integrity of records created by chromatographic data systems:
1. Identify each user uniquely
2. Implement adequate password controls
3. Establish different user roles / access privileges
4. Establish and maintain a list of current and historical users
5. Control changes to the system
6. Use only trained staff to operate the system
7. Understand predicate rules for laboratory records
8. Define and document e-records for the system
9. Review the audit trails for each run
10. Back the system up regularly

Smith[11] has discussed the potential data integrity issues associated the use of Fourier transform infra-red (FTIR) spectroscopy to identify drug substances. The usual process is to obtain the spectrum of the batch being tested and then to compare this with a reference an authentic reference spectrum. The preparation of some types of sample for FTIR identification, such as KBr or nujol mull, can require some practice before an acceptable spectrum can be obtained. In light of this, it has been common practice to reject infra-red spectra prior to comparison if they do not comply with certain requirements. However, this practice could be interpreted as the spectroscopic equivalent to test injections on a HPLC system, and could be difficult to defend.

The current paper is the first part of an ongoing series which will discuss data integrity in regulated and accredited environments. Part one of this series will present a discussion of the

fundamentals and principles of assuring data integrity. The second part will discuss strategies for establishing systems to manage the integrity of laboratory data and records in regulated and accredited environments. The third part of this series will discuss the services that David Trew Consulting and/or Stericycle GXP Systems can offer. Subsequent papers will discuss developments in the subject as and when they occur.

## 2 Fundamentals of Data Integrity

The enduring assets of an organisation's operations are the records that document those activities. These records are often used to support critical decisions, such as:

- Regarding the quality of medical products for release into commercial distribution, which could affect the health of patients
- In support of national or international trade
- Concerning the safety of using chemical substances in consumer products, or
- Regarding prosecution of criminals

The reliability and trustworthiness if those records are of paramount importance.

In addition, if records are used to perform a regulatory function, they are considered to be legal documents. Falsification of, or even wrongly making changes to, such records can be considered criminal acts, and could result in criminal exposure for the person performing those acts[11].

For records to be considered reliable and trustworthy they must comply with the following fundamental attributes: Legible, Attributable, Contemporaneous, Original, Accurate, Complete, Consistent, Indelible and Available. In addition, it is submitted that verifiable is also a fundamental requirement.

### 2.1 Legible and understandable

A record that cannot be read or understood has no value and might as well not exist. All records should be composed so they conform to grammatical convention which should be consistent throughout. It is best to avoid buzzwords, cliques and slang as these are prone to change with time and are often not understood outside a particular locality. It is always good practice to have any record reviewed by a second person as this can often highlight any ambiguities.

### 2.2 Attributable

All data generated or collected and records must be attributable to the person generating the data or making the record. This should include who performed an action or created a record and when the activity was performed or the record created. For paper records this is normally done by the individual signing and dating the record with their signature. For electronic records, each user must have an individual account for their exclusive use. Access controls must be implemented which prevent access to anyone other than the authorised user. The use of computer accounts by anyone other than their authorised users will undermine the ability of the organisation to attribute a record to its originator. In addition, it could also be considered fraud and my result in criminal exposure.

As the records being signed may be legal documents, it is critically important that signers clearly understand the meaning of, and implications associated with their signatures. A signature, whether it is a traditional handwritten signature or an electronic signature, should be individual to a specific individual and the practice of signing someone else's name or initials is fraud, and is taken very seriously.

## 2.3 Contemporaneous

Contemporaneous means to record the result, measurement or data at the time the work is performed. Delaying writing up, for example until the end of the day, will inevitably affect the accuracy of that record as details can be forgotten or miss-remembered. For electronic records, entries should be accompanied by a date and time stamps which should flow in order of execution for the data to be credible. Data must never be back dated.

## 2.4 Original

All records must be original; information must be recorded directly onto the document or entered directly into the computer system. This avoids the potential of introducing errors in transcribing information between documents. If information from a computer system is printed out, that printout should be signed, dated and attached to the record. However, the electronic record is the original record.

## 2.5 Accurate

The record must reflect what actually happened. Any changes should be made without obscuring or obliterating the original information, the use of whiteout or correction fluid is prohibited. Any changes made to a record should be signed by the person making the change and dated to show when it was made and a written explanation should also be provided. Remember, the record may be needed after you have left the company and cannot be contacted for clarification.

## 2.6 Complete

The record must contain all information associated with the analysis of the sample, including system suitability tests, injection sequences, processing methods, sample preparation procedures and results. This must also include any reinjections or repeat analysis performed on the sample. Remember the position of the regulatory authorities for something that needs to be done is – 'if it isn't documented it's a rumour'. However, failing to disclose reanalysis or reinjection of samples will undermine confidence in the reliability of the records.

## 2.7 Consistent

Consistency in this context refers to the sequence of the component events, which the analytical method comprises, being performed in a logical order. For example, it is not possible to commence a HPLC run before the samples have been prepared, therefore the balance printout for the sample weights should be date/time stamped prior to the sample injection time. Therefore, all date/time stamps should be in the expected sequence.
In order to avoid confusion in this respect, it is worth ensuring all instruments that produce date/time stamped printouts are synchronised. This is best done by reference to a standard reference time, such as a national online time server.

## 2.8 Indelible

Indelible means the record must be legible for the lifetime of the record and once it has been made it cannot be removed.

- Hand written entries of information should be made in ink and not pencil which can be erased.
- If printouts are made on thermal paper, which darkens with time, a photocopy should be made; this should be certified as an accurate copy of the original print and attached
- If print outs are attached to a page they should be
  - Secured to the page as specified in your laboratory's SOPs
  - Signed and dated across the attachment and the page
  - Annotated with a reference to the document

## 2.9 Available

All records should be available for inspection, audit and review for the lifetime of the document. If a document is requested during a regulatory audit, it should be produced within thirty minutes. Therefore, the laboratory should establish an easy to reference archive system. Records should be archived so as to preserve their integrity, such as

- Secure facility with restricted access
- Effective fire suppression
- Protection from dampness or humidity
- Controlled access to Document

## 2.10 Verifiable

In the current data integrity environment, it is not sufficient to have reliable and trustworthy data, you must be able to convince a sceptical audience of regulators and other stakeholders of the integrity of your data. It is therefore, critical to establish mechanisms whereby the fundamental attributes, discussed above, can be verified. This includes capturing metadata, such as an audit trail, which clearly establishes when the record was created and who created it. It addition, it is also critical to establish that the data retains its original content. If changes have been made then the audit trail should capture who made the change, when the change was made and why the change was made. When entering an explanation for a change it is important to provide a meaningful explanation. Words like update, revision or correction do not convey any useful explanation. It is important to explain why the update, revision or correction was made.

# 3 Principles of Data Integrity

The World Health Organisation has identified some principles for assuring the integrity of data and records with will be discussed here. Good management data and records are critical components of a pharmaceutical quality management system (QMS). A systematic approach will provide a high level of assurance that all GxP records and data are accurate, consistent, trustworthy and reliable throughout their lifecycle. The QMS should include policies and procedures that address the following general principles of a good data management program.

## 3.1 Applicability to both paper and electronic data.

The data and record management program must assure robust control of data validity of both paper and electronic data and records. Reverting from an automated or computerized to manual or paper-based systems does not remove the need for robust management controls.

## 3.2 Applicability to all Contractual Parties.

These principles apply to parties to a contract. However, it is the purchasers, clients or users who are ultimately responsible for the robustness of all decisions made on the basis of GxP data, including those that are made on the basis of data provided to them by the party preforming the services or providing the data under the terms of a contract. Purchasers, clients or users should therefore perform due diligence to assure themselves that the service provider has appropriate programmes in place to ensure the trustworthiness and reliability of the data provided.

## 3.3 Good Documentation Practices.

Good documentation practices (GDP) should be followed to ensure all records, both paper and electronic as this allows for the full reconstruction of the related activities. In addition, GDP ensures that robust decisions are made based on reliable and complete data sets.

## 3.4 Data Management Programs.

To establish a robust and sustainable good data management system it is important that senior management ensure that appropriate data management programmes are in place.

The critical components of an effective management program should include:

- The application of modern quality risk management principles and good data management principles to the current quality management system to integrate those elements that assure the reliability of data. This could include monitoring the risks associated with data integrity and applying appropriate quality metrics. This can provide management with the necessary oversight for good decision making that will reduce the risks of data integrity failures.
- Personnel must be free of any commercial, political, financial and other pressures or incentives that may adversely affect the quality and integrity of their work;
- There must be adequate human and technical resources allocated to avoid excessive workload and pressures on those who are responsible for generating data and for keeping records, which may increase errors;
- Staff must be made aware of the importance of their roles in ensuring data integrity, and the importance of these activities in assuring product quality and protecting patient safety.

## 3.5 Quality Culture.

A quality, no blame, culture should be established and maintained in the working environment. This minimises the risk of non-compliant records and erroneous records and data. In addition, it also minimises the incentive to conceal errors and non-compliance.

An essential component of this is the transparent and open reporting of all deviations, errors, omissions and aberrant results at all levels of the organisation. Steps should be taken to prevent, detect and correct weaknesses that are identified with systems and procedures that

may lead to data errors. In addition, this will also lead to improved decision making processes.

## 3.6 Quality Risk Management and Sound Scientific Principles.

In the current quality environment, the resources allocated to controlling the reliability and trustworthiness of data and records should be consummate with the assessed risks associated with a lack of integrity for the particular data or records. Risk assessment tools, such a Failure Mode and Effects Analysis (FEMA), can be applied to evaluating the risks associated with a failure in data integrity

Robust decision making processes that rely on valid and complete data, must be supported by effective quality risk management systems, and also by the application of sound scientific and statistical principles. For example, the scientific principle of being an objective, unbiased observer regarding the outcome of a sample analysis. This requires that any suspect results must be first be investigated in a though, timely and unbiased manner. A suspect result should only be rejected if there is convincing evidence that clearly identifies a cause. Good data and record-keeping principles requires that any rejected results be recorded, together with a documented justification for their rejection, and that this documentation is reviewed and retained.

## 3.7 Data Lifecycle Management.

There are many potential lifecycles that particular data or records could be subject to. Often this will depend on the nature of the data or record. From a data integrity perspective, it is necessary to define data lifecycles and then identify the risks to data integrity at each stage during that lifecycle. A lifecycle management plan can then be developed to manage and control those risks

In addition, to ensure that the organisation, assimilation and analysis of data and its subsequent transformation into information that facilitates evidence based and reliable decision-making; the data management program should address ownership of data and assign responsibilities for the data management processes and risk management throughout the data lifecycle.

## 3.8 Design of record-keeping methodologies and systems.

Record-keeping methodologies and systems, whether paper or electronic, should be designed in a way that encourages compliance with the principles of data integrity. Examples include but are not restricted to:

- Identifying an appropriate time standard and restricting access to changing clocks for recording timed events;
- Ensuring batch records are accessible at locations where activities take place, so that *ad hoc* data recording and later transcription to official records is not necessary;
- Controlling the issuance of blank paper templates for data recording so that all printed forms can be reconciled and accounted for;
- Restricting user access rights to automated systems in order to prevent changes being made to both data and audit trails;
- Ensuring automated data capture or printers are attached to equipment such as balances;
- Ensuring proximity of printers to relevant activities;

- Ensuring ease of access to locations for sampling points (e.g. Sampling points for water systems) such that the temptation to take shortcuts or falsify samples is minimized;
- Ensuring access to original electronic data for staff performing data checking activities.

### 3.9 Maintenance of record-keeping systems.

The systems implemented and maintained for both paper and electronic record-keeping should take account of scientific and technical progress. Systems, procedures and methodology used to record and store data should be periodically reviewed and updated as necessary.

## 4 Conclusions

There can be little doubt that, in a regulated or accredited environment, issues with the reliability and trustworthiness of laboratory data and records can have extremely serious consequences for the laboratory's customers, management and staff. In light of this it is vital that everyone working in a regulated or accredited environment that creates records or data must understands the principles and fundamentals of good data integrity practice, which have been discussed in this paper.

However, understanding the principles and fundamentals of good data integrity practice is insufficient on its own to assure the reliability and trustworthiness of records and data. In addition, staff and, in particular, management must also be able to apply these principles and fundaments and develop management strategies to assure the integrity of records and data. This will be the subject of the second paper in this series.

## 5 References

1. MHRA, *MHRA GMP Data Integrity Definitions and Guidance for Industry*, Mar 2015, http://www.cyclonepharma.com/Guideline/MHRA.pdf, Accessed 28 Jun 2017,
2. MHRA, *MHRA GMP Data Integrity Definitions and Guidance for Industry – Consultation Document*, Jul 2016, https://www.gov.uk/government/news/mhra-gxp-data-integrity-definitions-and-guidance-for-industry, Accessed 28 Jun 2017
3. FDA, *Data Integrity and Compliance with CGMP Guidance for Industry*, Draft Guidance, Apr 2016, https://www.fda.gov/downloads/drugs/guidances/ucm495891.pdf, Accessed 28 Jun 2017
4. WHO, *Guidance on Good Data and Record Management Practices*, Draft Guidance, Sep 2015, http://www.who.int/medicines/areas/quality_safety/quality_assurance/Guidance-on-good-data-management-practices_QAS15-624_16092015.pdf, retrieved 28 Jun 2017
5. PIC/S, Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, Draft Guidance Aug 2016, https://picscheme.org/en/news?itemid=33, Accessed 28 Jun 2017
6. R.D. McDowall, *FDA's Focus on Laboratory Data Integrity – Part 1*, http://www.scientificcomputing.com/article/2013/09/fda%E2%80%99s-focus-laboratory-data-integrity-%E2%80%93-part-1, Sept 2013, Accessed 26 Aug 2016
7. FDA, Warning Letter WL: 320-13-17, Issued to RPG Life Sciences Limited, 28 May 2013

8. R.D. McDowall, *FDA's Focus on Laboratory Data Integrity – Part 2*, http://www.scientificcomputing.com/article/2013/09/fda%E2%80%99s-focus-laboratory-data-integrity-%E2%80%93-part-2, Sept 2013, Accessed 27 Aug 2016
9. US District Court for the District of Maryland, 25th January 2012, Ranbaxy Inc. and named individuals, Consent Decree of Permanent Injunction, Civil Action number JFM12CV0250
10. R.D. McDowall, *Ensuring Data Integrity in a Regulated Environment*, http://www.scientificcomputing.com/article/2011/05/ensuring-data-integrity-regulated-environment
11. P. Smith, *Data Integrity in the Analytical Laboratory*, *Pharma. Tech*., 2014, **38**, (5) 58 – 60, http://www.pharmtech.com/data-integrity-analytical-laboratory