DATA INTEGRITY

MAKE SURE THIS HOT TOPIC DOESN'T BURN YOU… OR YOUR SUPPLIERS, CONTRACT MANUFACTURERS OR CONTRACT LABORATORIES

by Maxine Fritz, George Toscano and Darren Jones

How confident are you that there are no data integrity issues within your firm, or within the many suppliers, contract laboratories or contract manufacturers you use in the development, manufacture and supply of your products or services?

There has been a noticeable increase in the past year or so in the number of significant enforcement actions taken by regulators, particularly the US FDA and the UK MHRA, related to data integrity. These have included the refusal to accept new product filings and the refusal to allow products to be marketed if manufactured at a site with known data integrity issues.

Over the years, there have been many previous data integrity-related issues that have tainted our industry. Current enforcement trends suggest that certain firms have failed to take heed of the history and importance of this topic.

The term **data integrity** is broad and may have widely different meanings depending on the specific context. In this article, the scope of "data integrity" is limited to pharmaceutical quality control laboratories, an area where many high profile data integrity problems are found, though the concept could easily apply to any electronic storage system or part of the supply chain utilized at a pharmaceutical manufacturer. This article provides an overview of some of the different types of and concerns regarding data integrity.

Any unintended change to data as the result of a storage, retrieval or processing operation (including malicious intent, unexpected hardware failure and human error) is a failure of data integrity.

Data integrity is an issue currently receiving plenty of attention from both the US Food and Drug Administration (FDA) and the UK's Medicines and Healthcare Products Regulatory Agency (MHRA). Although data integrity issues are not new, companies are being cited more frequently during inspections for observations related to data integrity, and agencies are even relying on evidence of data integrity issues from other regulatory bodies as the basis for taking enforcement actions against a pharmaceutical manufacturer.

Section 801(a) of the US Federal Food, Drug and Cosmetic (FD&C) Act states, "If it appears from the examination of such samples or otherwise" that an article is misbranded/adulterated, then the "article shall be refused admission" to the US It is this "or otherwise" phrase that enables the FDA to rely on other regulatory agencies' findings. Specifically, the Regulatory Procedure Manual (RPM), Chapter 9-6 Detention Without Physical Examination (DWPE), explains that DWPEs can be enacted when "an inspection conducted by FDA or by foreign or other government authorities under a Memorandum of Understanding (MOU) or other agreement" reveals evidence of non-compliance with FDCA 801(a). FDA has a "confidentiality commitment" with MHRA which enables the agencies to share non-public information about drug products, including any data integrity concerns. This confidentiality commitment specifically mentions cooperation between FDA and MHRA to "assist the other in conducting its regulatory functions."

As part of their standard inspection process, FDA and MHRA verify the accuracy and validity of various data, with a heightened focus on quality control activities. Relatively simple checks on systems and records frequently identify significant concerns, which are

▶▶

particularly pervasive with older data handling systems where more manual intervention is permitted. Cases of deliberate falsification of results and manipulation of data to make a failing result meet acceptance have been discovered – a GIANT RED FLAG to the regulators about a firm's quality culture.

The two sections highlighted present some common data integrity concerns found throughout pharmaceutical quality control laboratories, and provide recommendations for preventing potential breaches in data integrity.

COMMON DATA INTEGRITY ISSUES FOUND IN CHEMISTRY LABORATORIES:

Audit Trails – For electronic data acquisition systems, audit trails are not available or are not enabled; therefore, there is no record of data modifications or deletions. Surprisingly, companies are still cited for not enabling the audit trail feature on their software systems, even though this is a simple but powerful guard against data integrity issues.

Unique User Logins – Each user should have a unique username and password for both the analytical software and the operating system. This is essential for tracing work performed to a unique individual, and is critical for Good Manufacturing Practice (GMP) compliance and data integrity. Companies are often cited for having multiple users share the same username and password or, worse yet, having all users logging in as the administrator with privileges that may include the ability to modify or delete data.

User Privilege Levels – Each data acquisition system should have defined user levels based on the role the user will have in the system. Examples of common user levels include analyst, supervisor, manager and administrator. Privileges assigned to each level should be clearly defined and commensurate with the requirements for each user type. Examples of privileges include the ability to create methods, modify integration parameters, reprocess data and modify data.

Unofficial "Test" Injections – Some firms have been cited for injecting samples prior to beginning an official sequence. This practice results in essentially generating data for products, but not reporting the data.

Control Over Processing Methods – Use of high performance liquid chromatography (HPLC) processing methods (including integration parameters) that are not defined or controlled. This includes the practice of manual integrations without justification or approval, and processing injections in the same sequence with different processing methods and integration parameters. Another example of this practice includes processing standards that are used for quantitation of samples with different processing methods (integration parameters) without justification provided.

Control Over Electronic Systems – Failure to establish adequate controls over computer systems to prevent unauthorized access or changes to electronic data. This can include failure to have mechanisms to prevent unauthorized user access to the system, and ability to rename, move, delete or not save file results. Mechanisms should be in place to ensure that files cannot be accessed outside the analytical software (e.g. via the operating system) and edited, moved, renamed or deleted.

COMMON DATA INTEGRITY ISSUES FOUND IN MICROBIOLOGICAL LABORATORIES:

Traditionally, microbiological laboratories have relied on manual testing and recording operations, which opens the door to significant issues with data integrity. The issues observed often relate to the falsification of data; for example, recording fewer contaminants from a sample to ensure that the result meets the specification is a simple data integrity problem. How can a manufacturer be sure that company or contract laboratories are not guilty of falsification of data? Reviewing data trends can provide useful indicators – unlikely scenarios such as purified water systems with no microbial excursions or clean rooms with no environmental monitoring excursions are simple triggers that should prompt further investigation. If it looks too good to be true, it may well be! Spot checks of samples

▶▶

against the recorded results can also provide a good benchmarking indicator of whether there should be any concern regarding the integrity of recorded data.

Microbiological samples are often read and then rapidly discarded, so it is sometimes difficult to obtain evidence of falsification. Physical spot checks of samples in the incubator can be a powerful technique; if, for instance, physical spot checks identify the "first four purified water excursions ever" to be found on a site, it is likely these are not the first excursions.

Microbiological data patterns can also identify data integrity and falsification with a simple review of the data. For example, media growth promotion results can yield interesting patterns; there have been instances where only even numbers of colonies were recovered (apparently to make the averaging of the duplicate samples easier). When looking at growth promotion testing, it is often worth checking that the specification limit calculations have been performed and applied correctly. These are often found to be incorrect, resulting in missed out of specification (OOS) results. If something looks odd in the data, investigate it in detail, obtain supporting evidence, monitor results in the incubator over the course of the test and look at historic trends to assess data integrity.

A final recommendation for any quality control laboratory, whether chemistry or microbiology, is to be vigilant with laboratory paperwork. A recent case contained different versions of OOS investigations; the formal investigation that went for approval contained only one failed result, whereas a second unofficial and unapproved version recorded more excursions that appeared to have been hidden and not reported.

Overall, the crucial component to any data integrity review is to ensure that data is recorded exactly as intended and, upon later retrieval, ensure that the data is the same as it was when it was originally recorded. In short, data integrity aims to prevent unintentional changes to information, eliminating the potential for significant data integrity errors occurring in the pharmaceutical manufacturing process.

Evaluating a firm for data integrity issues requires a specific skill set and consulting/auditing toolbox, often not held within many pharma firms.

ABOUT THE AUTHORS

Our authors have significant experience of working with data integrity, both as regulatory inspectors (Maxine with FDA, Darren with MHRA) and all as consultants.

Maxine Fritz has 25+ years of combined FDA, industry and consulting expertise and is responsible for overseeing the Pharma Biotech practice at NSF Health Sciences.

George Toscano has more than 20 years of experience helping companies in the global pharmaceutical, biologic and biotechnology markets develop and execute comprehensive quality systems solutions. He is a recognized data integrity expert and has conducted numerous audits and assessments to evaluate companies' systems.

Darren Jones has 25 years of experience in pharmaceutical auditing, consulting and regulatory inspection support and preparation. Prior to joining NSF, Mr. Jones worked at MHRA where he spent four years as a GMP inspector.

For more information, contact **pharmamail@nsf.org** or visit **www.nsfpharmabiotech.org**

Cite as: NSF International. June 2017. Data Integrity. NSF: York, UK.

NSF INTERNATIONAL | PHARMA BIOTECH

The Georgian House, 22/24 West End, Kirkbymoorside, York, UK YO62 6AF

T +44 (0) 1751 432 999 | **E** pharmamail@nsf.org | www.nsf.org | **www.nsfpharmabiotech.org**