Data integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality.

A robust data governance approach will ensure that data is complete, consistent and accurate, irrespective of the format in which data is generated, used or retained.

An increased focus on data integrity and governance systems has led to serious consequences for several companies. This is the first of a series of 3 blogs which will explore elements of organisational behavior and system design which can mean the difference between data integrity success and failure.

One of the top global issues reported in the pharmaceutical media over the past 2 years has been data integrity. Regulatory actions resulting from data integrity failures have led to the withdrawal of supply across multiple markets, product recall, and serious reputational damage for those companies concerned. However this hot topic is not a new requirement, as basic data integrity principles are already described in international good manufacturing practice guidance.

There is a general misconception that data integrity failures only result from acts of deliberate fraud. Yet in the collective experience of my colleagues and me, the majority of issues relate to bad practice, poor organisational behaviour and weak systems, which create opportunities for data to be manipulated. However there is a way for companies to navigate the troubled waters of data integrity deficiencies by taking some basic behavioural, procedural and technical steps to significantly improve their systems.

1. Impact of organisational culture: is your company behaving well?

The impact of organisational culture and senior management behaviour on data governance must not be underestimated. Indicators with relevance to data governance provide a measure of the workforce's understanding and reporting behaviour, combined with the management's receptiveness to 'bad news'. Is error or system failure reported as an opportunity for improvement, or is there a mind-set around 'not wanting to cause trouble'? To remove the incentive to manipulate, re-create or amend data, the managerial response to 'bad news' must be fair and consistent, and not based on a fear of consequences.

2. 'Led from the top; empowered from below'

Organisational culture is not just addressed by senior management putting the right words in a mission statement. I have seen that communicating expectations clearly to staff at all levels in the company, and then living by these principles, is the key to success. Leadership, engagement and empowerment of staff at all levels in the organisation can then combine to identify and deliver systematic data integrity improvements where good practice becomes automatic.

As the philosopher Aristotle observed:

"We are what we repeatedly do. Excellence, then, is not an act but a habit".

3. The data lifecycle

With support from the correct organisational culture, the next important element of successful data governance is to understand the data lifecycle. This will enable the implementation of a system which is designed to assure the integrity of data throughout its life, beyond the limitations of data review.

The data lifecycle considers all phases in the life of the data, from initial generation and recording, through processing, use, archiving, retrieval, and (where appropriate) destruction. Failure to address just one element of the data lifecycle will weaken the effectiveness of the measures implemented elsewhere in the system.

4. Establishing data criticality and inherent integrity risk

In addition to staff training and implementation of data integrity policies, consideration should be given to the organisational (eg procedures) and technical (eg computer system access) controls applied to different areas of the quality system. The degree of effort and resource should be commensurate with data criticality (how it is used) and inherent risk (how it is generated).

Data which relates to critical process control, batch release decisions or longterm stability may have significant impact to product quality. Other data, while of relevance to the operation of a GMP compliant facility, may be of lower criticality.

The way in which data is generated will influence the inherent data integrity risk. Data may be generated by a paper-based record of a manual observation or, in terms of equipment, a spectrum of simple machines (eg pH meters and balances) through to complex highly-configurable computerised systems (eg HPLC and ERP systems). The inherent risks to data integrity will differ depending upon the degree to which data generated by these systems can be configured, and therefore potentially manipulated.

Our inspectorate finds that manufacturers typically focus data integrity and validation resources on large and complex computerised systems, while paying less attention to other systems with apparent lower complexity. Whereas simple machines may only require calibration, the data integrity risk associated with systems linked to user configurable software (eg PLC-linked production equipment and infra-red / UV spectrophotometers) can be significant, especially where the output can be influenced (modified or discarded) by the user. Without well designed controls it may be possible to manipulate data or repeat testing to achieve a desired outcome with limited opportunity of detection.

5. Designing systems to assure data quality and integrity

A mature data governance system adopts a ‘quality risk management’ approach across all areas of the quality system. It requires continuous review, proportionate risk-reduction measures, and an understanding of residual risk across the organisation. Despite recent high-profile regulatory cases regarding falsification of analytical data, the collective experience of the MHRA Inspectorate is that data governance is not limited to laboratories or computerised systems. There are opportunities to strengthen both paper and computerised elements of the data lifecycle.

A useful acronym when considering data integrity is ALCOA; data must be attributable, legible (permanent), contemporaneous, original and accurate. The expectations for designing systems which reduce opportunities for data integrity failure are described in more detail in guidance published by MHRA. Simple (and often low cost) system design can have significant impact on the success of data governance. Some are included below as indicators of the ALCOA principles.

5.1. Attributable

The identity of the person completing a record should be unambiguous. The use of aliases or abridged names should only be permitted where this is consistently used, and attributable to an individual. The same alias or IT system log-in which cannot differentiate between different individuals should not be used.

5.2. Legible (permanent)

It should not be possible to modify or recreate data without an audit trail which preserves the original record. It is important not to forget paper records in this context. Blank forms for manual recording of data should also be controlled in a manner which prevents unauthorised re-creation.

Exceptionally, there may be a valid reason to re-create a record, eg where it has been damaged beyond use, or where an error does not enable a GMP compliant correction of the original. This must be managed through the quality system, either by making a ‘true copy’ (verified as being a true replicate of the original), or by re-writing a new copy and

retaining the original as evidence. In all cases, this must be approved through the quality system, with QA oversight and justification for the action.

It is generally accepted that correction fluid is not acceptable in GMP areas. However, companies may be unaware that their computerised systems often have 'data annotation tools' enabled. These permit changes to data which can alter the appearance of reports, and may not have a visible audit trail. From a practical perspective, this is 'electronic correction fluid', and should not be permitted.

5.3. Contemporaneous

System design has significant impact upon contemporaneous record keeping. The availability of records in the right place at the right time removes the need for staff to use loose scraps of paper, or their memory, to retain information for retrospective completion in the official record.

When inspecting packaging operations, I still find it a common approach for manufacturers to use a single batch packaging record (BPR) for blistering and cartoning of a solid dosage form. However, if the BPR is located in the secondary packing area, it is impossible for staff in the primary packing area to make contemporaneous records, and vice versa. The BPR may also require periodic checks, such as equipment performance. Specifying exact time intervals (eg 'every 60 minutes') may result in an incentive for staff to 'back date' the time of the check if they were occupied at the exact time the activity was required. The system is encouraging staff to falsify the record, particularly if there is concern that missing an exact time point might lead to disciplinary measures.

This can be addressed by 2 simple changes. Specifying an acceptable window for completion of the activity (eg.'every 60 ±5 minutes'), and splitting the BPR into 2 parts (primary and secondary) encourages the correct behaviour, and removes both opportunity and incentive to falsify the record.

5.4. Original

Original records must preserve data accuracy, completeness, content and meaning. Metadata (data about data) is vital in this aim by enabling reconstruction of an activity – who did what, where and when. There are certain limitations in relation to file formats which may not maintain the full metadata record; so-called 'flat files' such as .pdf, .doc etc. We may know who created the file, and when, but there may be no information on how, when or by whom the data presented in that document was created, processed or amended. There is therefore an inherently greater data integrity risk with flat files, as they are easier to manipulate and delete as a single record with limited opportunity for detection.

5.5. Accurate

Automated data capture, with the required IT controls, provides greater control over the accuracy of a record. Where automation is not possible or feasible, real-time second operator verification of quality-critical observed values may be necessary.

Data review must include a review of raw data in its original form. If access to electronic raw data is not possible remotely, this is a good opportunity for the reviewer to escape the confines of their office. Reviewing paper copies or flat file reports of electronic data, even from a validated secure system, is unlikely to enable detection of anomalies. This is because the preparation of reports still requires operator intervention, which can influence what data is reported, and how it is presented.

6. Trial (injections) and error

The use of 'trial injections' in chromatographic tests to verify stability of the analytical set-up is a recurrent theme reported as grounds for regulatory action. This practice is particularly concerning where the 'trial injection' is a product sample, whose results are then discarded or retained under a different file structure to other results. In these circumstances, data integrity is undermined, particularly if the result obtained from the trial injection failed to comply

with specification. At the very least it asks serious questions regarding analyst understanding of data integrity, quality system design or managerial response to undesirable results.

In cases where analyses run over an extended period, it may be understandable that the analyst would wish to verify that the analytical system is operating as expected before committing the full system suitability and sample set. Where there is management agreement that verification of analytical system stability is required prior to system suitability checks, there are some basic considerations which can address the data integrity concerns.

The practice needs to be consistent with the company's data governance system. The system stability check must be proceduralised as part of the approved method or standard operating procedure (SOP), with corresponding guidance on the assessment of the results, and all data (including system stability check samples) should be reported. Importantly, a sample of the product batch under test should not be used for the system stability check. An independent, well-characterised sample or standard will fulfil the analytical requirement without raising data integrity concerns relating to 'testing into compliance'. A robust laboratory data governance approach will also include periodic reconciliation of analytical sample runs, to confirm that there are no concealed trial injections or modified sample runs.

7. Supply chain

In the first blog of this series I described how omitting one aspect of the data lifecycle weakens the effectiveness of other governance measures. The same principle applies to the supply chain. A failure at one site weakens all sites downstream in the chain.

To keep the supply chain moving, organisations need to place reliance on summary reports – batch records, analytical data, validation reports etc, especially in relation to outsourced services. It is therefore important to use supplier audits as an opportunity to build confidence in these summaries provided on a routine basis. What is the contractors organisational culture and maturity relating to data governance? What systems do they have to ensure data integrity?

8. Conclusion

Data governance is an integral part of the pharmaceutical quality system, with effort and resource being balanced in accordance with other risks to product quality. As such, manufacturers and analytical laboratories are not expected to implement a forensic approach to data checking on a routine basis, but instead design and operate a system which provides an acceptable state of control based on data criticality and inherent risk.

Data integrity requirements apply equally to manual (paper) and electronic data. Reverting from computerised to paper-based systems will not in itself remove the need for data integrity controls. The implementation of effective behavioural, procedural and technical steps based on a clear understanding of risk will ensure that the system will encourage the right behaviours, improve compliance, and provide greater assurance of product quality.

9. References

- Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 1 - David Churchward, 25 June 2015 (https://mhrainspectorate.blog.gov.uk/2015/06/25/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-1/).
- Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 2 - David Churchward, 14 July 2015 (https://mhrainspectorate.blog.gov.uk/2015/07/14/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-2/).
- Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 3 - David Churchward, 27 August 2015 (https://mhrainspectorate.blog.gov.uk/2015/08/27/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-3/).