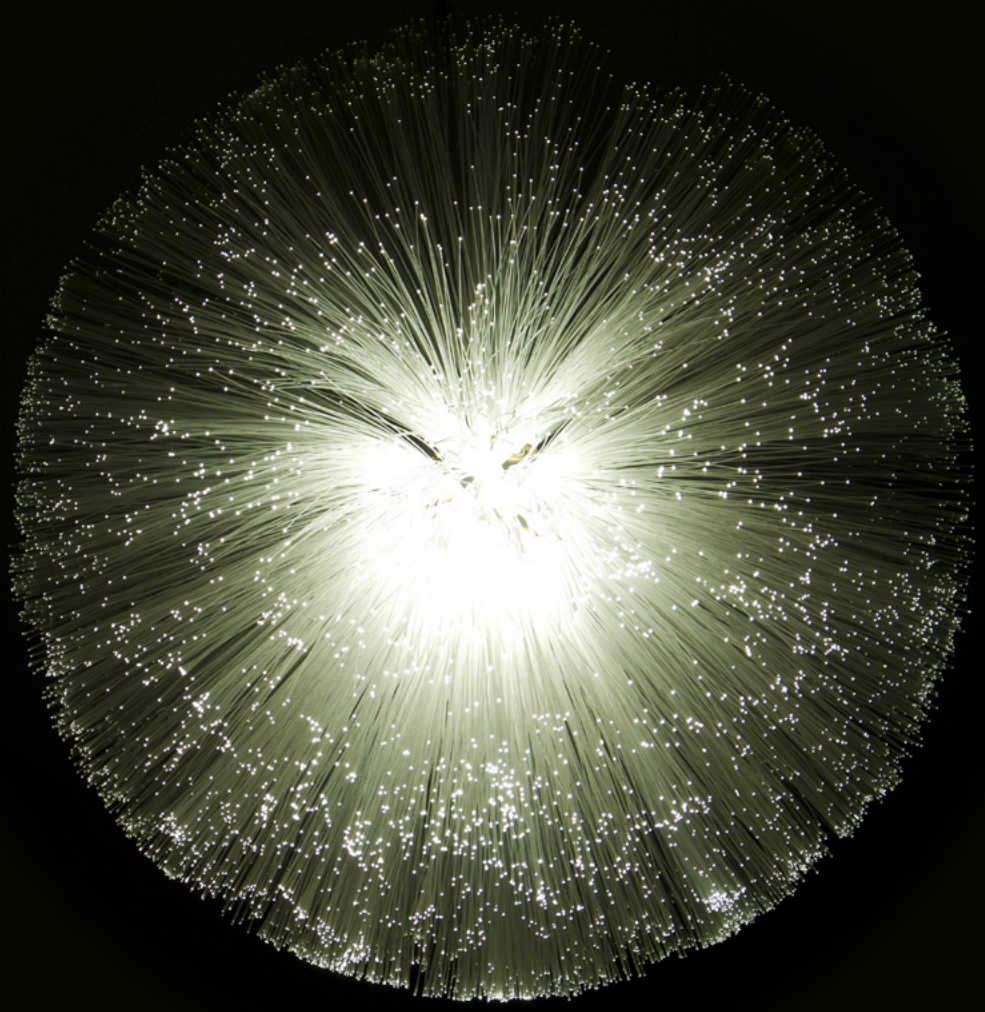
Deloitte.



Under the spotlight

Data Integrity in life sciences

Introduction

Summary

The integrity of data generated by highly regulated life sciences companies is critical, because properly recorded information is the basis for manufacturers to assure product quality, safety and efficacy prior to product approvals and subsequently placing them onto the markets for human use.

Data Integrity is also important for quality control procedures during manufacturing to ensure patient safety. As global regulatory focus on Data Integrity increases, companies that fail to comply may face penalties ranging from public warning letters to criminal charges and product removal from the marketplace. In recent years there has been a significant increase in the number and types of issues related to data practices, including: unauthorised data access, lack of enabled audit trails, accidental and intentional falsification of records.

Regulatory bodies now have high expectations with regard to data quality and integrity owing to the life sciences industry's growth, globalisation and adoption of advanced technology, such as highly automated systems and storage of data in 'The Cloud'. The need to be compliant is expected to drive organisations to make significant changes to their current data-related processes and systems that require corporate-wide efforts and cross-functional collaborations. The implementation of good data practices requires consideration, not just of controls, processes, IT and clear roles and responsibilities, but of a wider shift towards education and a culture that understands and values Data Integrity.

What is Data Integrity?

According to the guidelines published by the regulatory bodies, Data Integrity is defined as the extent to which all data are complete, consistent, and accurate throughout the data lifecycle. Data here includes all original records and true copies, including source (raw) data, metadata and all subsequent transformations and reports of these data.[1, 2, 3, 4, 5]

Regulatory authorities expect paper and electronic data generated in the process of testing, licensing, manufacturing, packaging, distribution, and monitoring of medicines to be collected and maintained in a secure manner. The requirements for data include that they are attributable, legible, contemporaneous, original and accurate (ALCOA) (Figure 1).

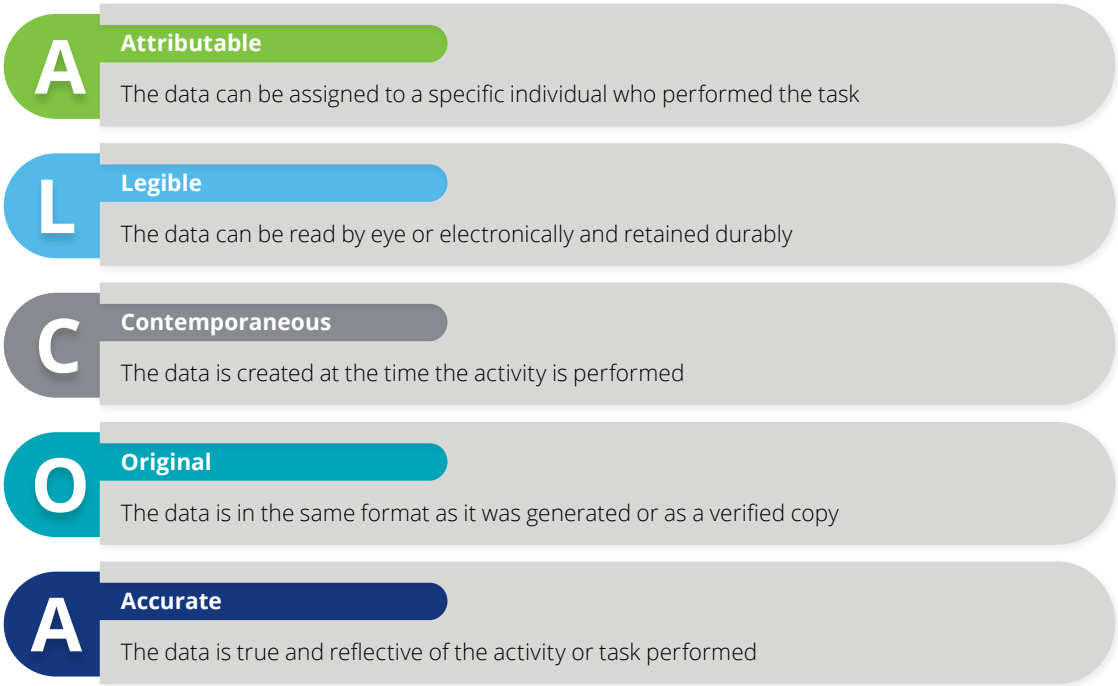


Figure 1: ALCOA characteristics of data

Implicit in the requirements for ALCOA are that data should be complete, consistent, enduring and available (usually referred to as ALCOA+).

In addition to ALCOA, there are standards for storage and backup, which must be applied equally to both electronic and paper-based data. Where paper data exists, it must be stored and backed up as securely as electronic data. Scanning paper data elements for backup is good practice, but must be performed utilising a validated process and controlled by verification of completeness. Where data retention is outsourced to an external party, the elements of the contract which relate to ownership and retrieval of data should be thoroughly understood, and the vendor should be qualified and managed like any other critical services vendor through established vendor management processes. It is important to realise that data are part of the Good Manufacturing Process (GMP) supply chain and must be treated with the same standards of quality.

The different guidelines produced by the various regulators are substantially harmonised with each other. Therefore, changes to data life-cycle management performed in order to comply with one of the guidelines automatically facilitates compliance with the other guidelines.

From the generation and processing of data to its storage and destruction, there are many components that contribute to compliance with regulations and international standards. Maintaining a high level of Data Integrity is multifaceted and requires not only strong policies and controls, but also staff training, segregation of duties and a culture of compliance. A typical data lifecycle beginning with the creation of data and ending in its deletion is shown in Figure 2 along with good data practices for each phase.[6]

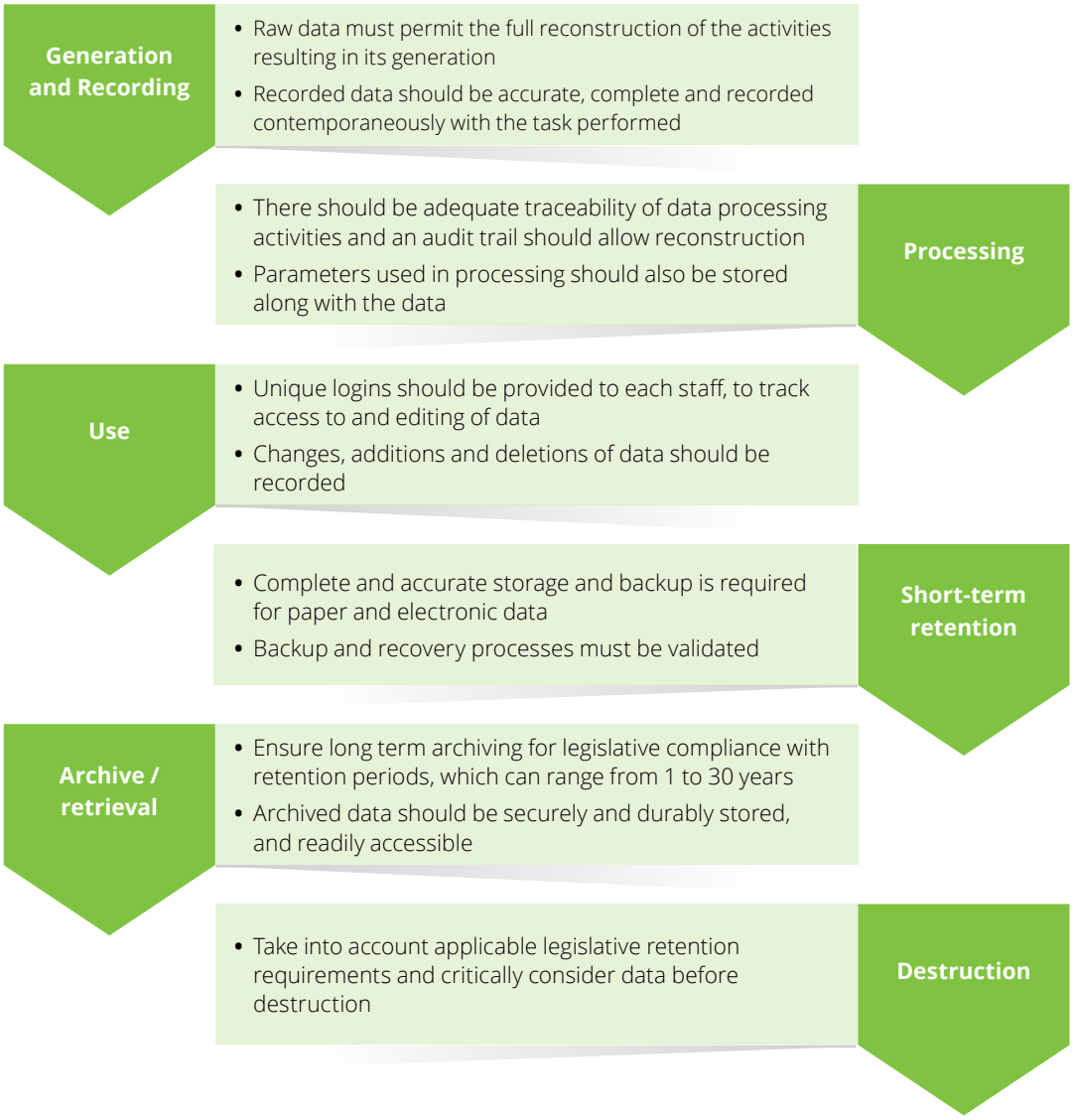


Figure 2: Typical data lifecycle and good practices for each stage

Why is there an increasing focus on Data Integrity compliance by regulators?

In recent years, there has been an increase in the number of violations in data manipulation and other data issues in pharmaceutical manufacturing facilities, particularly ones based in Asia during GMP inspections by the regulators. Between 2013 and 2015, there were over 15 Data Integrity warning letters issued by the regulatory agency to the pharmaceutical manufacturers in India alone. [7, 8, 9]

In 2016, a regulatory agency issued 75 warning letters for a range of violations including unlawful promotion, insufficient registration, unlawful distribution, scientific violations and manufacturing quality violations. Of these letters, 43 percent contained instances of Data Integrity violations (Figure 3).[10]

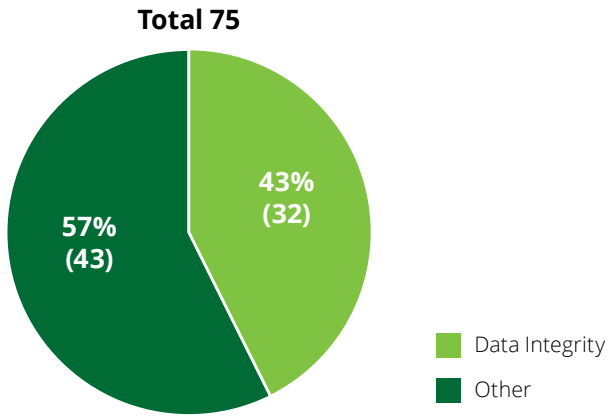


Figure 3: Percentage of total FDA warning letters issued in 2016

These warning letters were heavily skewed towards manufacturers in Asia, which accounted for 72 percent of 32 data related warning letters issued globally, with the remainder being spread across Europe and Americas (Figure 4).[11]

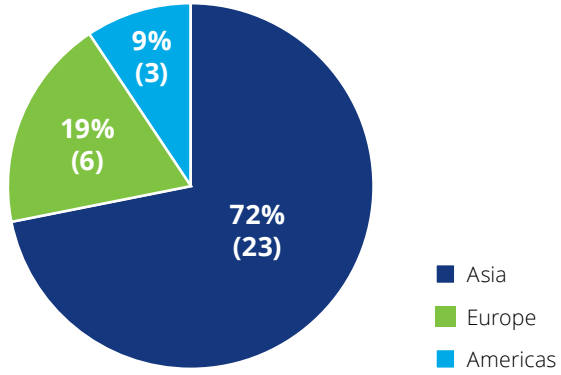


Figure 4: Data Integrity related warning letters issued in 2016 by the regulatory agency

The relevant warning letters were issued for a range of different reasons, most commonly due to data not being fully and accurately documented, which accounted for 34 percent of the violations (Figure 5).[12]

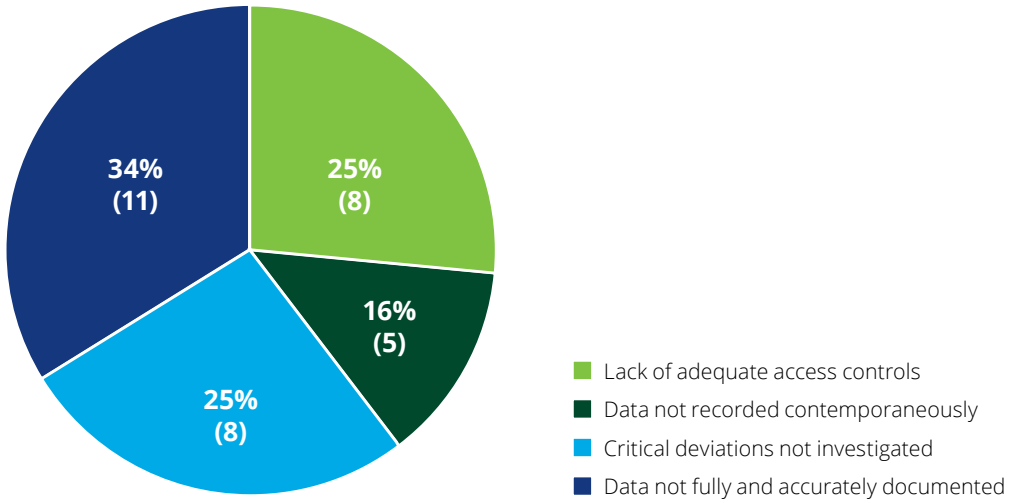


Figure 5: Breakdown of the 32 Data Integrity violations brought up in warning letters in 2016

Due to such frequent violations of basic Data Integrity practices, regulators globally are focusing on enforcing principles and practices to ensure product quality and patient safety.

Why is it difficult to get Data Integrity right?

There are a range of challenges faced by life science organisations attempting to implement good data practices. These include:

- Inadequate processes, technology and controls - life science organisations must implement appropriate measures and controls in business processes and IT systems, such as validation of a process or an IT system, to ensure data is generated timely and accurately. Without adequate measures in place across the data life cycle, the integrity of data can be compromised.
- Insufficient training and awareness – employees often experience a high volume of training sessions in a short period of time and it is estimated that up to 75% of training may be worthless. This could result in staff members not able to fully understand all the requirements and standards relating to Data Integrity. In other cases, training materials are of poor quality and/or members of staff miss some of the training sessions due to heavy workloads.[13]
- Data Integrity is not embedded into the corporate culture - the impact of organisational culture and senior management behaviour must not be underestimated. A culture that values good data practices must be led from the top and empowered from below. Management teams should lead by example by communicating company standards as well as expectations to all levels of staff.
- Business and performance pressure - in today's business environments employees are expected to multi-task and deliver in short-spaces of time for assigned tasks. Staff members may, under time and performance pressure, cut corners in order to complete the tasks assigned without considering the consequences that the generated data may bring.
- Outsourcing and contracting - companies outsourcing work have responsibility for the integrity of all data involved, including those maintained by any subcontracting organisation or service provider. In addition to having their own data governance systems, companies that outsource activities should also verify the adequacy of comparable systems at any subcontractors and providers of relevant computing services, such as contracted IT data centres, database support personnel and cloud computing solutions. The responsibility of an organisation to maintain Data Integrity across its extended enterprise can provide significant challenges in the assurance and monitoring of data quality.

Common Data Integrity violations

As part of their standard inspection process, regulatory agencies verify the accuracy and integrity of various data, with an increasing focus on quality control activities. As discussed above, a number of recent warning letters have highlighted such concerns. Issues noted in these letters encompass many of the elements highlighted in recent guidance. These issues include, and are not limited to, the following:

- *"Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established API specifications and standards."* In the example, this failure included the discovery of residual solvent testing data in the Recycle Bin folder, and failure to retrieve test data upon request.[14]
- *"Failure to prevent unauthorised access or changes to data, and failure to provide adequate controls to prevent omission of data."* This failure, in one case, included the discovery that chromatography metadata (e.g. time and date) could be changed without the changes being reflected in the audit trail. In another case, analysts deleted unknown peaks without justification, making the drugs in question appear to conform to their specifications. One of these peaks was for a residual solvent known to be a genotoxic impurity.[15]
- *"Failure to record activities at the time they are performed and destruction of original records."* In one case, this failure involved the backdating of batch production records, and the destruction of original records after being manually transcribed.[16]
- *"Failure to train employees on their particular operations and related GMP practices."* In the example, this included the declaration by employees that they had not received training for their production operations. The company in question was not able to produce any training reports for inspectors, despite the generation of training reports being part of company policy.[17]

What are the consequences if Data Integrity is failing?

As noted above, following recent GMP inspections, violations and failures have resulted in a range of regulatory actions, including warning letters, import alerts and product detentions. Current guidance indicates that failures in Data Integrity can result in the following regulatory and non-regulatory consequences[18]:

- Frequent inspections or suspension of product approvals - when regulatory issues arise, they are likely to result in loss of regulatory trust. This can result in more frequent inspections of the facility, a requirement to see more data to support claims, and may make it unlikely for a company to obtain approvals from the regulatory authority.[20]
- Import bans, forced recalls, plant shutdowns, debarment - for serious violations, products which have Data Integrity issues are considered by the regulatory agency to be adulterated. As such, if they are shipped to the USA, the regulatory agency can prevent them from being allowed into the country. Additionally, they can mandate that the product be recalled or subject to seizure. Health Canada has also imposed restrictions, quarantines and recalls due to Data Integrity concerns based on the findings of other regulatory bodies. The regulatory body can, at its own discretion, punish even technical violations which may not result in obvious threats to patient health. In addition to warning letters, the available enforcement actions include approval withdrawals, plant shutdowns, injunctions or penalties and debarment of individuals. The regulatory body has also resorted to suspending drug sales when it discovered that the integrity of the underlying data was compromised.[21, 22, 23]
- Criminal enforcement - the New England Compounding Centre manufactured drug products that resulted in a number of individuals dying from meningitis. During an inspection by a regulatory agency, the investigators found numerous cases of negligence and Data Integrity issues, for example, falsified cleaning logs to show cleaning was performed when it was not performed. Following the investigation, criminal charges were filed against 14 employees from high level executives to operators in the clean room. Conviction on these types of charges can result in prison terms in addition to large fines.[24]
- Loss of reputation and public trust - the publication of warning letters in newspapers and consumer domains, can significantly tarnishes the reputations of a company. This may result in a loss of public confidence in those companies affected and lead to a loss of business. There have recently also been high profile warning letters from the regulatory body for serious GMP violations which can result in adverse publicity.[25]
- Lack of strategic data insights - the industry is seeing a push towards using generated data not just for regulatory compliance and quality assurance, but moreover to gain strategic insights into their businesses. Weak standards of Data Integrity will compromise the potential of an organisation to generate value and a competitive advantage through data driven decision making.

Approach to Data Integrity compliance

As pharmaceutical organisations adapt to achieve compliance, they should expect to drive significant changes to the current processes and systems, ushering in a new era of cross-functional collaboration.

Due to the evolving regulatory landscape, the development of new technologies and changing ways of working from mostly manual to electronic, organisations should ensure that they have appropriate measures in place to ensure all data is consistent and accurate. These measures apply to both manual and electronic data generation and should be commensurate with differing levels of risk.

Data Integrity requires a cohesive, integrated and organisation-wide program in order to succeed. While it crosses many functions, roles, services and even business units, it cannot be treated in a fragmented and haphazard manner. A piecemeal approach to compliance can lead to gaps, inefficiencies, and poor security throughout the product lifecycle. When implementing a programme to identify, develop, review and improve Data Integrity across an organisation, a focus on standardisation and procedures, risk assessment, technology and systems, and data governance will be essential. These steps should be part of a larger cultural shift driven by engagement and education. (Figure 6).

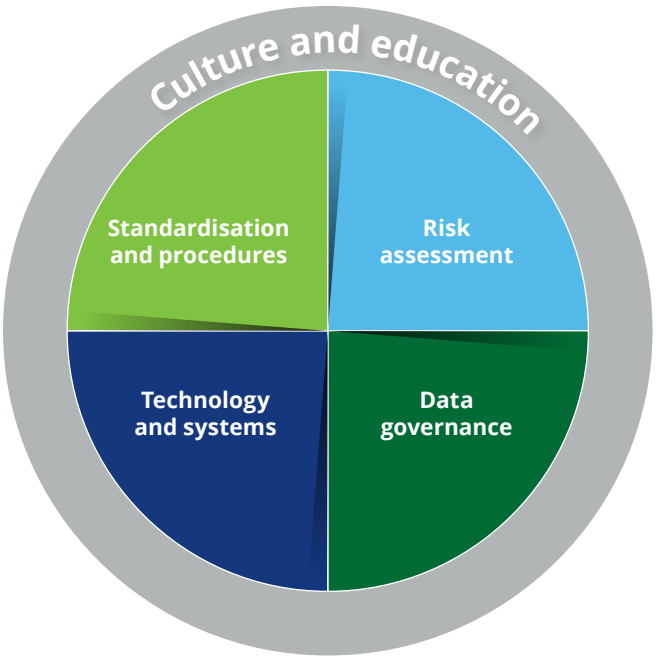


Figure 6: Approach to implementing Data Integrity across an organisation

Education and culture

The impact of organisational culture on the success of data governance measures should not be underestimated. Regulators now expect the industry to be proactive in its efforts to implement good Data Integrity practices, rather than just react to inquiries or defend themselves if audited. It is imperative that all employees and contractors fully understand the importance of their responsibilities with respect to data collection, processing and management. They should also understand how to identify data concerns when they arise, how to resolve them and where to seek advice and support when needed. There should be a channel for employees and contractors to make suggestions for continual improvement

and management. This should promote the creation of a working environment that encourages an open reporting culture. Companies also need to understand the impacts that their decisions and actions may have on the products and subsequently patient safety if they ignore Data Integrity issues.

With the need for continuous improvement, companies must progress towards creating a corporate culture focused on quality and compliance. Company leadership and senior management should embrace and exemplify best practices while cascading awareness and understanding of the requirements throughout the organisation.

Standardisation and procedures

To create a common understanding of data integration requirements and expectations, organisations should review available regulatory documents including official regulations, industry guidance and definitions from leading regulatory bodies. These regulatory documents should be interpreted and implemented into an organisation's business processes, procedures and policies. Process optimisation should be at the forefront of implementing new processes to ensure that business value is maximised simultaneously with regulatory compliance. There must also be a standardisation of the contracting process with regards to Data Integrity requirements from and obligations of the third party.

Risk assessment

Conducting a gap analysis of business processes, equipment and systems against regulatory requirements and expectations will provide results for risk assessment and prioritisation. In particular, risk assessment techniques, such as ICH Q9 Quality Risk Management, should be used to determine the importance of each data processing step by effectively monitoring data criticality (impact to decision making, product quality and safety) and data risk (vulnerability of data to alteration, deletion or loss) at each stage of the data lifecycle. When analysing the identified risks, the focus should be on reviewing the current controls of data in a process, procedure or a system in order to identify any weaknesses and minimise the risks.

Technology and systems

As paper-based data have been moving online, the requirements for different IT systems and databases should be defined. Data Integrity concerns should be tackled as part of a broader technology risk management strategy that addresses data security, application controls, cyber risk and IT operational management. Critical issues include having clear roles and responsibilities with corresponding access privileges, as well as unique logins to enable the audit trail function that records all actions taken by each person. Audit trails should also be reviewed at pre-defined intervals that commensurate with differing levels of risk. It is important to recognise that data relating to a product or process may cross various boundaries during their lifecycle (between IT systems and organisational applications, as well as storage) and regulators will require evidence that Data Integrity is maintained throughout.

Companies need to further assure that their products have been manufactured according to recognised and validated protocols and that all related information is properly recorded, traceable and reported. Only such information can help to ensure the quality, safety and efficacy of products before they are distributed to the market.

Data governance

Developing and implementing a global governance committee in an organisation is important. This global governance committee should be responsible for developing a Data Integrity strategy and common standards across the organisation. Additionally, it should be responsible for monitoring practices within the organisation and throughout the extended enterprise, including third party contractors. Data governance measures should ensure that data is complete, consistent and enduring throughout the whole data lifecycle. Also, data governance needs to address data ownership, support the design, operation, review and monitoring of data-related processes. At local levels, subject matter experts should provide specific advice and recommendations for improvement opportunities, whilst business process and system owners should monitor and manage their Data Integrity performance.

Conclusion

The growing issues of Data Integrity across life science companies means that organisations need to be able to adapt rapidly to prevent violations and regulatory consequences. Good data practices will enrich the quality of data, allowing companies to make strategic decisions backed by analytics and data-driven insights. To enable this, companies will need to provide sufficient training to their employees, develop assessment and monitoring programmes, as well as establish Data Integrity as an integral part of the internal audit programme. Such changes are essential to developing a culture that values data quality with an awareness of and focus on GMP. Companies that fail to develop and implement suitable standards risk falling behind global regulatory requirements and may face consequences ranging from recalls and plant shutdowns to criminal charges, in addition to losing the competitive advantage of valuable data insights.

References

1. http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp&mid=WC0b01ac05800296ca#
2. http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM495891.pdf
3. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf
4. https://picscheme.org/en/news?itemid=33
5. http://www.gmp-compliance.org/guidemgr/files/WHO_TRS_996_ANNEX05.PDF
6. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf
7. India's Data Integrity Problems, RAPS 03 February 2015
8. US FDA Inspections in China: An Analysis of Form 483s from 2015, RAPS 10 February 2016
9. http://www.fdanews.com/topics/111-data-integrity
10. http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCompanies/ucm482462.htm
11. Ibid
12. Ibid
13. https://www.forbes.com/sites/groupthink/2015/08/30/why-your-employee-training-is-a-waste-of-time-and-money-and-what-to-do-about-it/#788f044028cf
14. http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2016/ucm528590.htm
15. Ibid
16. http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm455345.htm
17. Ibid
18. http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM495891.pdf
19. Ibid
20. Data Integrity in Pharmaceutical Industry: Journal of Analytical & Pharmaceutical Research 2016, 2(6): 00040
21. http://www.hc-sc.gc.ca/dhp-mps/pubs/compli-conform/tracker-suivi-eng.php
22. https://www.dlapiper.com/en/us/insights/publications/2016/05/the-writings-on-the-wall/
23. http://www.fdanews.com/topics/111-data-integrity
24. 14 Indicted in Connection with New England Compounding Center and Nationwide Fungal Meningitis Outbreak Wednesday, Department of Justice, Office of Public Affairs December 17, 2014.
25. https://www.bloomberg.com/news/articles/2017-01-24/shredding-paper-before-fda-visit-raises-india-compliance-queries

Contacts

David Hodgson

Partner
DTTL Global LSHC Risk Advisory Leader
davhodgson@deloitte.co.uk

Fiona Maini

Director
Deloitte UK
fmaini@deloitte.co.uk

William Greenrose

Advisory Managing Director
Deloitte United States
wgreenrose@deloitte.com

Sinja Christiani

Director
Deloitte Switzerland
sichristiani@deloitte.ch

Sarah Chan

Senior Manager
Deloitte UK
sachan@deloitte.com

Balazs Hargitai

Assistant Manager
Deloitte Switzerland
bhargitai@deloitte.ch

Acknowledgements

Gagan Arora

Jai Dongre

Namita Pai

Deloitte.