www.ThePharmaJournal.com

The Pharma Innovation

ISSN: 2277- 7695
TPI 2017; 6(2): 110-115
© 2017 TPI
www.thepharmajournal.com
Received: 18-12-2016
Accepted: 19-01-2017

Jain Sanjay Kumar
Nirma University, Chandlodia,
Gota, Ahmedabad, Gujarat,
India.

Correspondence
Jain Sanjay Kumar
Nirma University, Chandlodia,
Gota, Ahmedabad, Gujarat,
India.

Strategy to avoid data integrity issues in pharmaceutical industry

Jain Sanjay Kumar

Abstract

Data integrity is vital for the pharmaceutical industry and organization shall be able to demonstrate the integrity of the data during regulatory audits. Review of various warning letters revealed that there are compromises w.r.t. data integrity and have resulted into serious implications on the organization including import alert and debarment of the employees.

It is always better to proactively prevent issues, such as data integrity failures to occur, than trying to remediate and resolve inspection findings. Compliance excellence makes good business sense.

This document provides the regulatory requirement, graphical summary of the issues in recent past through review of warning letters, suggest the strategy to prevent the data integrity breaches by design, by procedural control and monitoring.

Keywords: Data integrity, ALCOA, Warning letters, Validation, Audit Trails

1. Introduction

Data integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality as decisions on product quality are made based on the data. Electronic data and computerised systems have introduced new challenges to maintain data integrity; hence the data governance system should be integral to the pharmaceutical quality system as required by regulatory authorities. The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands. As such, manufacturers and analytical laboratories shall 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.

Data integrity requirements apply equally to manual (paper) and electronic data. Manufacturers and analytical laboratories should be aware that reverting from automated / computerised to manual / paper-based systems will not in itself remove the need for data integrity controls.

The regulatory authorities have put much emphasis on data integrity in recent years because they uncovered serious cases of data integrity breaches. It is always better to proactively prevent issues, such as data integrity failures to occur, than trying to remediate and resolve inspection findings. Compliance excellence makes good business sense.

This document provides the regulatory requirement, graphical summary of the issues in recent past through review of warning letters, suggest the strategy to prevent the data integrity breaches by design, by procedural control and monitoring.

1.1 Regulatory Requirement

Data integrity is critical to regulatory compliance. USFDA has published the 21 CFR Part 11 and EU has published Annex 11 to spell out the requirement with respect to computerised system. 21 CFR Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in Agency regulations [1]. EU GMP Annex 11 applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together full fill certain functionalities. The application shall be validated; IT infrastructure shall be qualified.

Where a computerised system replaces a manual operations, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process [2].

Both FDA and MHRA use the acronym ALCOA to define its expectations of electronic data [1, 3].

Attributable – Who acquired the data or performed an action and when

Legible – Data can be easily read

Contemporaneous – documented at the time of activity

Original – written printout or observation or a certified copy thereof

Accurate – no errors or editing without documented amendments

In addition, definition of data integrity that FDA uses for internal training is: "Data are of high quality if they are fit for their intended uses in operations, decision-making and planning. as data volume increases, the question of internal consistency within data becomes paramount…."

For decision of safety, there must be rigorous and thorough application of fundamental scientific practices, irrespective of the purpose of study [4].

Indeed, this is essentially its role in the pharmaceuticals industry – associated with recording data about good manufacturing practices, the creation and manipulation of the data base records, storage and any other activity that requires accountability within or of the organization [5].

1.2 What is Data Integrity?

MHRA guidance has defined Data are complete, consistent and accurate throughout the data lifecycle [3]. The integrity of data can be assured only in the absence of bias. Data integrity can be found in virtually any aspect of pharmaceutical manufacturing. Bias has no place in pharmaceutical science. Breach of Data Integrity means introducing Bias which can be deliberate or can be accidental, however either way, it can be detrimental to the Quality System [6].

Data Integrity means state when data has not been altered in an unauthorised manner. Data Integrity covers data in storage, during processing, and while in transit. Tentative Definition for Falsification in Relation with GMP Inspection (EU) by Dr Thomas HECKER in his one of the presentation is "Any wilful mis-statement, misrepresentation, manipulation, adulteration, rewriting, hiding, replacing of quality related documents, materials, activities or buildings in order to give an item the appearance of GMP compliance when this is not the case, as these facts are not isolated and/or known, approved / supported by management (e.g. false analytical data checked and approved) [7]."

1.3 Generic Drug Scandal

In 1989, a major scandal erupted involving the procedures used by the FDA to approve generic drugs for sale to the public. Charges of corruption in generic drug approval first emerged in 1988, in the course of an extensive congressional investigation into the FDA. Investigation discovered that several manufacturers had falsified data submitted in seeking FDA authorization to market certain generic drugs. In April 1989, the FDA investigated 13 manufacturers for irregularities; and Dozens of drugs were eventually suspended or recalled by manufacturers [8].

At the outset of the generic drug scandal uncovered in the late 1980's FDA developed an administrative Application Integrity Policy. At or about the same time, legislation (the Generic Drug Enforcement Act [GDEA] of 1992), provided for debarment of individuals convicted of certain misdemeanor or felony offenses. This meant that an individual that was convicted could be debarred permanently from providing directly or indirectly any services in any capacity to a firm in the pharmaceutical industry. This is interpreted to include any service (including cutting the grass) if employed by a pharmaceutical company.

During the generic drug scandal, there were 22 criminal convictions of drug companies and 70 convictions of industry and FDA personnel as well as $50 million in fines levied against these organizations and individuals. Eventually there were some 70 individual debarment actions relating to the shenanigans that occurred but to date no firm has been debarred under the provisions of the GDEA.

Following are the number of debarments looked like over the last few years.

Table 1

Year	Number of Debarments
2013	4
2012	13
2011	18

Most of the debarments seen now are either for clinical investigators that have falsified study records, individuals that have engaged in the distribution of unapproved drugs or those that have perpetrated mail fraud or some other type of fraud. One must remember that debarment can be permanent or permissive (with a defined period of time usually from 5-10 years).

So even after the lessons of the past, there are some that continue try to beat the system, perform illegal activities or fraudulently create data for their own gain or the gain of others. The saying that history has a tendency to repeat itself appears to be true when speaking of issues that could result in debarment. We need to learn from the past before it is forgotten [9].

1.4 Review of Warning letters issued by FDA related to data integrity

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 [15].

Author reviewed the FDA website[10] and identified that total 59 Warning Letters were issued worldwide to the pharmaceutical industries from Jan-2012 to Jun-2014. These are further categorized as below -

- API Manufacturing = 12
- Finished Pharmaceuticals =46
- Testing Laboratories = 01

1.5 Observations are classified as

1. **Laboratory Control Observations:** The observations related to laboratory control are sub-classified as depicted in the Fig 1. Most of the observations are pertaining to breach of data integrity in the laboratory e.g. unauthorized changes in electronic data, falsification of

data, false data recording, lack of computer system control, unofficial testing, trial injections etc.

2. **Manufacturing control and Quality System Observations:** The observations related to laboratory control are sub-classified as depicted in the Fig 1. Most of the observations are pertaining to breach of data integrity in the manufacturing e.g. Torn GMP documents found in the waste bin, unofficial batch record, lack of computer system control etc.

Most of the companies who found engaged in the data integrity issues, FDA has issued them import alert notification means these companies cannot further export the products to US market till the issues are resolved to the satisfaction of USFDA.

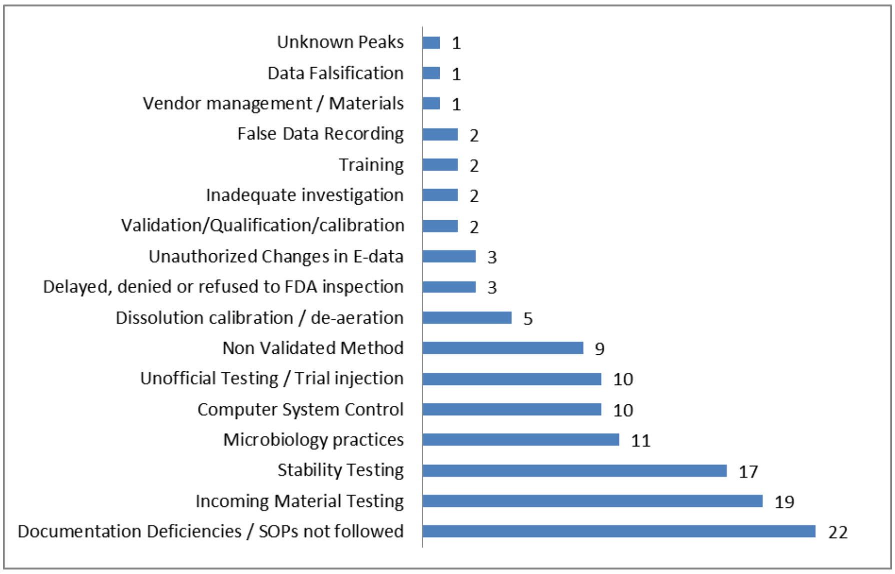

Fig 1: FDA Warning letters - Laboratory Control Observations

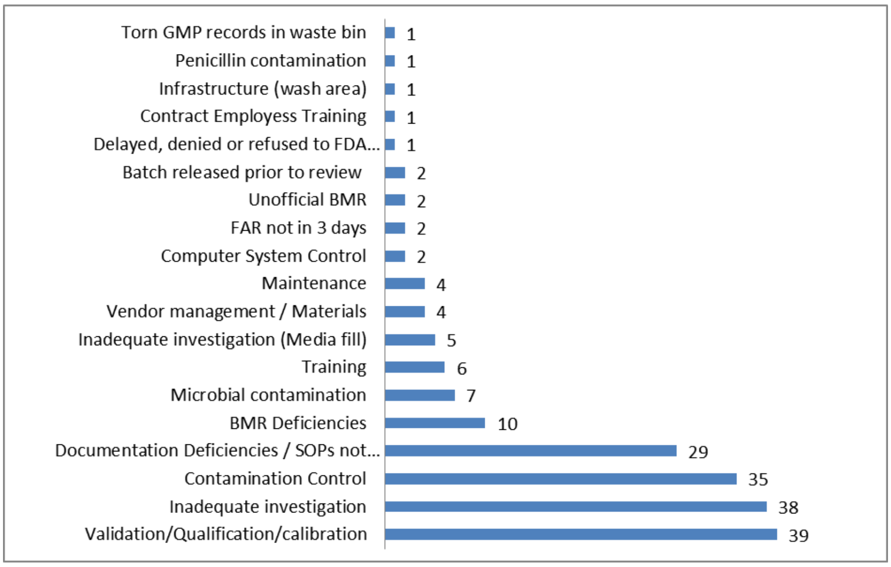

Fig 2: FDA Warning letters - Manufacturing control and Quality System Observations

Summary of the observations raising question about data integrity are as below -

1. Page replacement / Unofficial documentation
2. Falsification of Data
3. Not reporting the OOS/ Failures
4. Person not available for activities
5. Machine not available, but batches executed
6. Blank training records
7. Blank signed calibration record from vendor

1.6 Consequences of data integrity issues

Data integrity issues may result into warning letters, import alerts and penalties to the organization. To the individuals who are involvement in the wrong doings, it can be debarment and imprisonment.

1.7 Strategy to avoid data integrity

Pharmaceutical companies need to ensure that all the data generated during the manufacturing and testing of the drug products are original, accurate, correct and integral. Given the increased scrutiny for data integrity, companies are well advised to establish internal competency, assessment and monitoring programs [11].

Following are the recommendations to establish three level system to avoid any data integrity issues and avoid any regulatory impact during the audits -

1. **Building and Sustaining the Quality culture in the organization**

There is a general misconception that data integrity failures only result from acts of deliberate fraud. 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 [15].

Culture is symbolic communication. Some of its symbols include a group's skills, knowledge, attitudes, values, and motives. The meanings of the symbols are learned and deliberately perpetuated in a society through its institutions.

A quality-focused culture –

- Creates a healthy work environment
- Develops people
- Enables managers to guide effectively
- Staff feels that their efforts are worthwhile
- Leads to satisfied customers

In one of the presentation of Mr. Mag Oliver has described the principle of the quality culture as below [12].

- Empowering the stakeholders to develop their own quality goals, initiatives and measures
- Guaranteeing transparency and common standards without succumbing to a purely formal quality approach
- Showing trust without disregarding the risks involved
- Strengthening reciprocal communication process balancing the delegation and acceptance of responsibility

Additionally, Management shall ensure that it is transparent, accountable and involved (continuous and actively). It set realistic expectations from the employees and practices fair praise and criticism of the employees.

Organisational culture is not just addressed by senior management putting the right words in a mission statement but 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 [15].

2. Control By design

Without well designed controls it may be possible to manipulate data or repeat testing to achieve the desired outcome with limited opportunity of detection [15].

The European Medicine agency (EMA) GMP requirements for the computer systems are contained in Annex 11: Computerised systems. The guidance provides consistent criteria for effective implementation, control and use of computer systems in GMP-regulated activities. Annex 11 may be applicable for software used in the production of a device (e.g. PLC is manufacturing equipment) and software used in implementation of the devices in quality control system (e.g. software that records and maintains the device history record). A computer system must ensure that the methods for record keeping and retention allow at least the same degree of confidence as that provided by paper based systems [2].

The basic EMA requirement on data integrity comes from EU council directives 2003/94/EC and 91/412/EEC. “The electronically stores data shall be protected, by methods such as duplication or back-up and transfer on to another storage system, against loss or damage of data, and audit trails shall be maintained.”

The following controls maintain the data integrity as part of the life cycle of the system:

a) Validation: Validation of computerized systems and the extent of the validation, take into account the impact the systems have on the ability to meet predicate rule requirements. One should also consider the impact those systems might have on the accuracy, reliability, integrity, availability, and authenticity of required records and signatures. Approach shall be based on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity.

b) Audit trails: There shall be computer- generated, time-stamped audit trails, for example - date, time, or sequencing of events, as well as any requirements for ensuring that changes to records do not obscure previous entries to ensure the trustworthiness and reliability of the records[1]. Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation. As part of ensuring data integrity, it is imperative to keep track of all changes made to information in the electronic records that document activities related to GMP-relevant records. The use of audit trails helps to confirm that only authorise additional, deletions or alternations of GMP relevant electronic record have occurred and allow a means to reconstruct significant details about manufacturing activities and data collections, this is necessary to verify the quality of the data and the data integrity [2].

Audit trails or other security methods used to capture electronic activities –

- Must contain any GMP-relevant electronic records are subject to all requirements regarding data integrity
- Should describe when, by whom, and the reason changes were made to the electronic record. Original information should not be hidden though the use of audit trails or other security measures used to capture electronic record activities.
- Must be available
- Must be regularly reviewed

Audit trails can be useful investigative tools. Examining audit trails for a specific set of records as part of an investigation where data integrity is uncertain, or as a component in data integrity review as part of an established business process, can be powerful tool to help determine the trustworthiness of the records [13].

c) Risk Management: Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

d) Personnel: Only authorized users be able to access a computer and the level of access to a computer system be based on the users’ assigned tasks.

e) Suppliers and Service Providers: Service providers include all parties who provide any services irrespective of whether they are employed by an external company, to the same company, or an internal service unit. The use of vendor-supplied software presents some additional difficulties in acquiring objective evidence of the quality of the software, hence it requires a level of knowledge sufficient to provide confidence in its accurate, consistent and reliable behaviour when employed by a specific user.

f) **Requirement Document:** User specification requires both structural and functional analysis which describes what functionality is required and the data integrity controls are needed to be implemented depending on the intended used of the computer system.

g) **Date Migration:** Data migration is the process of transferring data between storage types, formats or computer systems. It is a key consideration for any system implementation, upgrade or consolidation. If the data is transferred to another data format or system, the verification of the data migration should include corroboration that data are not altered in value, meaning, structure, context, and links (e.g. audit trail)

h) **Data storage:** Data storage refers to any device that records (Stores) or retrieves (reads) information (data) from any medium, including the medium itself. After the data is in the storage device, data integrity must be ensured. Logical and physical protections must be adequate to the criticality of the computer system. There must be a record of any data change, including the previous entry, who made the change and when the change was made. To reduce the risk of losing data and guarantee data availability to users, periodic back-ups must be performed and back-ups must be stored separate from the primary storage location. The efficacy of the back-up and restore processes must be verified as a part of initial qualification.

i) **Security:** Strong computer security is the principal way of protecting the integrity of electronic records. Only authorised personnel can make changes to any component of the computer system and assures the security of the records residing in the system. A defined procedure at network and application levels should be established for the issuance, cancellation, and alternation of authorization to enter and amend records, including the modification of the passwords. Periodic reviews must be performed after the initial validation. Electronic records should be verified, stored, backed-up and archived as part of the periodic reviews of accessibility, readability and accuracy. Back up output should be verified in order to ensure the accuracy of the audit trail data. Where a record is deleted prior to meeting the planned retention date, an audit trail of the deletion should be kept until the end of the approved retention period. Any instances where unauthorised persons attempt to access the computer system or data storage devices should be recorded.

j) **Incident Management:** Incorrect documentation, data errors, improper operation, and interface errors in computer system components, can affect the operation of a computer system. These events are known as non-conformances. These events shall be fully documented to evaluation & analyse to identify the root cause, to perform the impact assessment. Appropriate CAPA shall be initiated to avoid the recurrence.

k) **Business continuity:** Business continuity ensures continuity in the event of a system breakdown. It refers to the measure of preparedness that is required to ensure business operations in case of system failure or problem. The procedural controls needed to restore the system must be adequately documented and tested regularly.

l) **Electronic Signature:** Electronic records may be signed electronically and electronic signatures shall be permanently linked to their respective record and shall include date / time that they were applied.

m) **Printers with balances:** It is expected to use the printouts wherever weighing are performed in the laboratory as a part of the analysis. Printouts shall be attached with raw data duly signed / dated. Printers shall be protected to avoid any manipulation in changing the date / time.

3. Control By procedure

Remember that procedural controls are needed in the pharmaceutical organization. The following are title of the SOPs [14] that can be available with clear objective, defined responsibility and instructions to the users-

1) System Maintenance
2) Incident Management
3) Operational Change Management
4) Periodic Review
5) Data Backup, Archiving and Restore
6) Disaster Recovery
7) Security Management
8) Business Continuity Planning
9) Security Management
10) System Administration
11) Archiving and Retrieval

Issuance of record: Wherever paper based documentation practices exist, it is vital that issuance control and retrieval is under control of quality unit to avoid any manipulation in the documentation pertaining to manufacturing, analysis of the batches.

4. Control by Monitoring

a) **Independent review of records:** After execution of the analysis of the sample, it is recommended to have independent review of the raw data in the form of hardcopies against electronic records by independent experience team to ensure the correctness, accuracy and traceability of the data. There should be a procedure which describes the process for the review and approval of data, including raw data. Data review must also include a review of relevant metadata, including audit trail. Data review must be documented.

b) **Internal Audit:** Data integrity verification activities shall be embedded into internal audit process and shall be performed periodically. A few companies have taken potential data integrity issues seriously by starting internal investigation, incorporating data integrity assessments into their quality assurance oversight programs, and in some case, establishing a special data integrity office. Companies – even those in good standing with regulators – have initiated such activities regardless of existing or anticipated compliance concerns [11].

5. Training

Create awareness among staff so they can assist with this endeavour, and report concerns before they become full-fledged issues. Train the internal auditors to understand what to look for when detecting data integrity deficiencies [11].

Conclusion

Data integrity is vital for the pharmaceutical industry and organization shall be able to demonstrate the integrity of the data during regulatory audits. Review of various warning letters revealed that there are compromises w.r.t. data integrity and have resulted into serious implications on the organization including import alert and debarment of the employees. With proper strategy and planning, organization can avoid such issues by creating the quality culture, building controls by design and adequate procedure. Given the increased focus on data integrity during the audits, companies are advised to establish internal assessment and periodic monitoring by the quality unit. This shall ensure the trust and confidence of the regulators in the pharmaceutical organization and continuity of the business.

2. References

1. Guidance for Industry Part 11, Electronic Records; Electronic Signatures Scope and Application, U.S. Department of Health and Human Services Food and Drug Administration August Pharmaceutical CGMPs, 2003.
2. EU GMP Annex 11: Computerised system, revision 1.
3. MHRA GMP data integrity definitions and Guidance for industry, revision 1.1 March, 2015.
4. Good Laboratory practices and safety assessment by Richard A becker, Erik R Janus, Russell D White, Francis H Kruszewski and Robert E Brackett, Environmental Health perspective, 2009; 117(11):A482-483.
5. Electronic signatures in the pharmaceutical industry-wider issues dominate over the technical and practical by James Whitman, Records Management Journal. 10(1):35-48s.
6. Peter Baker’s Presentation, Assistant Country Director (Drugs), US FDA India Office, US Embassy – New Delhi.
7. Data Integrity in Manufacturing Records Multicentre International Data Integrity Workshop; Mumbai, 3/4 and 6/7 November Dr Thomas HECKER, EDQM Inspector Certification of Substances Division, EDQM, 2014.
8. https://en.wikipedia.org/wiki/Food_and_Drug_Administration.
9. Latchman Blog - Bob Pollock, 27 March, 2014.
10. http://www.fda.gov
11. http://www.ivtnetwork.com/article/data-integrity-fda-and-global-regulatory-guidance.
12. Presentation on developing a quality culture, The basic framework by Mr. Mag Oliver, March, 2008.
13. A risk Base approach to Audit trail by Randy perez, Chris Reid, and Sion Wyn, Pharmaceutical engineering, March / April, 2015
14. Good Automated Manufacturing Practices - A risk based approach to Operation of GxP Computerised Systems
15. 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 1, David Churchward, 25 June, 2015.