Computer System Validation CSV in Data Integrity Implementation Strategies for Pharmaceutical Industry

Alexis Colón Nazario
Master of Engineering in Manufacturing Engineering
Advisor: Edgar Torres, Ph.D.
Industrial and Systems Engineering Department
Polytechnic University of Puerto Rico

Abstract *— Computer System Validation CSV in Data Integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA). Due to the rise in cGMP violations involving data integrity during regulatory inspections, there have been issuances of many warning letter, import alerts and consent decrees. Electronic signature and record-keeping requirements as mentioned in 21 CFR Part 11 and apply to certain records, subject to records requirements set forth in Agency regulations, including parts 210, 211 and 212. Further, regulations for Computer System Validation CSV in data integrity issues occur mostly in quality laboratories and production areas and the causes vary due to personnel, equipment and management. The implementation of regulatory guidelines and standard operating procedures for data integrity, regular internal audits or surveillances and training will pave way for pharmaceutical industries to maintain Computer System Validation CSV in data integrity flawlessly.*

Key Terms *—ALCOA, cGMP Violations, CSV, Electronic Signature, Regulations, Training, Warning Letters.*

INTRODUCTION

Computer System Validation CSV in Data Integrity is the assurance that data records are accurate, complete, intact, and maintained within their original context, including their relationship to other data records and aims to prevent unintentional changes to information. It refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, including the usage of any system which stores, processes, or retrieves data. The definition applies to data recorded in electronic and paper formats or a hybrid of both, which is being followed in certain industries. Ensuring data integrity means protecting original data from accidental or intentional modification, falsification, malicious intent (fraud), or even deletion (data loss). Data integrity and security are closely linked to the 21 CFR part 11 for electronic records and electronic signatures.

RESEARCH OBJECTIVES

The main objective of this design project is to present a strategic approach and guidance that will contribute to the reduction in cGMP violations involving CSV & data integrity for the Pharmaceutical Industry.

RESEARCH CONTRIBUTIONS

This project supports the Company's goal of the implementation of regulatory guidelines and standard operating procedures for data integrity, regular internal audits or surveillances and training will pave way for pharmaceutical industries to maintain Computer System Validation CSV in data integrity flawlessly.

RESEARCH BACKGROUND

This design project was conducted to the implementation of regulatory guidelines and standard operating procedure for data integrity will pave way for pharmaceuticals industries to maintain Computer System Validation CSV in data integrity flawlessly.

Regulatory Enforcement Background - History of Data Integrity Focus

This focus on the history of data integrity represents an evolution over the past 30-plus years and addresses both changes in technology and learning from GMP inspections. Assurance of data integrity is a component of the larger category of data management and applies equally to paper records and electronic records. The "generics scandal" of the 1980's raised the issue of falsified data submitted to FDA in support of drug approvals. One outcome of this scandal was the shift in focus of the FDA pre-approval inspection (PAI) to evaluate raw laboratory data included in the marketing application and evaluate whether the site was capable of manufacture as described in the application. This scandal also prompted implementation of the Application Integrity Policy in 1991 which "describes the Agency's approach regarding the review of applications that may be affected by wrongful acts that raise significant questions regarding data reliability" [1].

In parallel, FDA recognized the increased reliance on computerized systems within the pharmaceutical industry. They developed and published 21 CFR Part 11, the final rule on Electronic Records and Electronic Signatures in 1997. In 2003 FDA published a Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application to address enforcement priorities. FDA continues to communicate their interpretations in compliance actions such as forms 483 and warning letters, podium presentations and on their GMP Q&A web site page.

As early as 2000, a warning letter issued to Schein Pharmaceuticals cited lack of control over computerized laboratory systems including lack of password control and broad ranging staff authority to change data. FDA issued a 15-page form 483 to Able Laboratories in New Jersey in 2005. Failing laboratory results were identified that were not reported, and among the observations was failure to review electronic data including audit trails. Three warning letters were issued to two Ranbaxy sites in 2006 and 2008 [1].

Based on these compliance actions, FDA announced a pilot program in 2010 to evaluate data integrity as part of routine GMP inspections. FDA planned to use the information gained from these inspections to determine whether revisions to Part 11 or additional guidance on the topic were necessary. FDA also committed to take appropriate enforcement actions on issues identified during the inspections. In the slide deck FDA stresses that they will "continue to enforce all predicate rule requirements, including requirements for records and record keeping. Enforcement actions of FDA in this area continue due to widespread problems.

Warning Letters, Data Integrity and Compliance Issues Abroad – Focus on India and China

FDA notes in the guidance that it is observing an increased number of violations involving data integrity in CGMP inspections, including instances of poor records, inadequate written procedures, and deficient systems for ensuring effective production processes and controls at manufacturing facilities all over the world. FDA inspections cite a range of serious deficiencies in how employees handle important records and documents. There are reports of records found in trash bins, data that do not match test results, data manipulation, sample retesting to achieve desired results, and deletion of undesirable results. These violations have led to warning letters, import alerts, and consent decrees, particularly at facilities in India and China.

Data integrity has become a more serious compliance problem at pharmaceutical manufacturing plants throughout the world. Over the past three years, as the FDA has increased inspections of offshore facilities, the agency has penalized a number of API manufacturers in India and China for cGMP violations, many of them involving data integrity. In some of the FDA inspection reports, quality control employees said that they were ordered by superiors to back date lab data, or to delete information and perform tests until

samples passed. Some of the companies whose plants were penalized were also put on an import ban list, preventing them from shipping products to the United States [1].

There are major differences between how FDA operates in the two countries, which collectively account for about 80% of the world's APIs. Unlike in India, it's become increasingly difficult for FDA to obtain visas for its inspectors in China and in 2014; FDA closed two of its offices in Shanghai and Guangzhou, China, and consolidated operations at its Beijing location. Six employees from the FDA's China office were scheduled to begin conducting inspections from January to March, FDA said, which would be a slight boost from a few months prior when FDA only had two inspectors overseeing the roughly 700 manufacturing facilities there [2].

Similarly, in India, FDA has plans to double the number of its inspectors there – from about nine to 19, though even if that number is actualized the agency would still be tasked with inspecting more than 500 manufacturing sites exporting products to the US. Concerns over how FDA can adequately track the drug and API supply chain is starting to worry Congress. In December, the House Committee on Energy & Commerce sent a letter to the US Government Accountability Office calling on the oversight office to investigate whether FDA can adequately monitor the manufacturers in India and China, which in the past have had a history of counterfeiting, adulteration, substandard manufacturing and data falsification [2].

And though both China and India have domestic pharmaceutical inspectors and regulators (China FDA and Central Drugs Standards Control Organization, respectively), the standards used for these inspections are not yet on par with FDA's. Following issues are commonly found by FDA inspectors during inspections in Indian companies regarding data integrity problems:

Backup of Data

In some companies FDA found that they do not have the facility of data backup and restore. USFDA regulations state that all electronic data should be secured. Backup should be taken periodically and it should be stored on server to make it secure and not on the computer it is connected to.

Sharing Login IDs

This is the usage of a colleague's login ID instead of theirs. It mixes the work done by the analysts and the analysis done by the individual analyst cannot be identified. FDA doesn't allow it and rights about it in questions and answers.

Audit Trails

In some companies, audit trail function is found in some instruments like HPLC, GC, and Spectrophotometer etc. but remains disabled. Audit trails must be active in all instruments those generate electronic data. 21 CFR describes details about audit trail and digital signatures.

User Access Rights

Some analysts in quality control have rights to access the analytical data and they can edit or delete it. It is unacceptable to the FDA because analyst can alter the results of the analyzed products. Access rights to delete data should be given to the data reviewer only. Results of any faulty branch or reanalysis must not be deleted from the system. Everything done on the instrument should be available in instrument log. Analysts should also not have rights to change the system date and time.

The growing number of regulatory citations directed at API facilities around the world. Because India and China supply 80% of the APIs used in US pharmaceutical production which are mostly commodity-type products, the US government has been questioning FDA's ability to monitor quality in Chinese and Indian plants, according to a February 2016 report in the Regulatory Affairs Professionals Society (RAPS) journal, Regulatory Focus. API manufacturing company executives believe that data integrity issues and perceptions that suppliers from other parts of the world are not sufficiently trained in current good manufacturing practices (cGMPs) are making a move to outsource more APIs manufactured in the U.S. and Europe [3].

According to the RAPS report, 41 manufacturing sites in China are now on import alert, five are on alert in Hong Kong, and 42 sites in India. In December 2015, RAPS reported, US representatives wrote to the US Government Accountability Office asking that it look into whether FDA could handle the load of inspections now required in India and China. The agency closed two Chinese offices in 2014 to consolidate activities in Beijing. In India, FDA plans to increase the number of inspectors from nine to 19 [3].

Over a period of seven fiscal years the number of warning letters issued by the FDA to drug manufacturers because of GMP deviations (21 CFR PART 211) are 41, which were referring to the deficiencies described in the corresponding paragraphs of Part 211. Since 2009, which had 27 warning letters there has been a strong increase and in fiscal year 2010 eight companies received a warning letter [3].

RESEARCH METHODOLOGY

The methodology to be followed for the Data Integrity Implementation Strategies for Pharmaceuticals Industries. Solving model called complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).

Data integrity – requirements for complete, consistent, and accurate data.

Throughout **cGMP.**

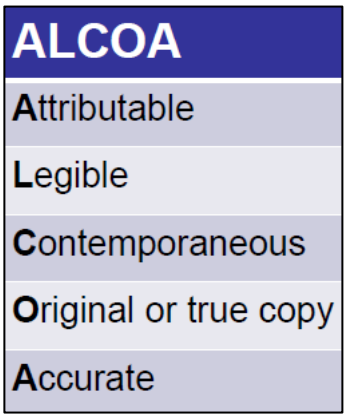

Figure 1 Terms of Data Integrity

Remembering – Verifying the integrity of your data means verifying that your data is:

- Reliable
- Consistent
- Accurate

Terms Associated with ALCOA

***Attributable* –** Who performed an action and when? If a record is changed, who did it and why? Link to the source data.

Legible – Data must be recorded permanently in a readable manner.

Contemporaneous – The data should be recorded at the time the work is performed followed by date & time stamps.

Original – It should be an original record and not a certified true copy.

Accurate – Errors should not be edited without appropriate documentation.

APIs – ICH Q7

Incidents related to computerized systems that could affect the quality of intermediates or APIs or the reliability of records or test results should be recorded and investigated.

Computerized Systems

- ***GMP* -** related computerized system should be validated.
- Appropriate installation and operational qualifications should demonstrate the suitability of computer hardware and software to perform assigned tasks.
- Incidents related to computerized systems that could affect the quality of intermediates or APIs or reliability of records or test results should be recorded and investigated.

Data Security

Within the scope of Computer System Validation CSV, Data Security is best defined as the act of protecting data against unauthorized access or corruption. Typically, not enough controls around computerized system is the root cause of data security issues.

Computerized System

A computerized system is any combination of hardware, software and associated infrastructure, that collects, creates, modifies, maintains, archives, retrieves, or transmits electronic data.

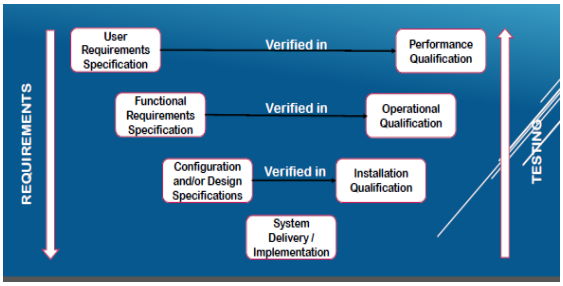

Figure 2
Computer System Validation V-Model

Data

"Computer data is information processed or store by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data".

Regulatory Guidance on CSV in Data Integrity

As per FDA: "the completeness, consistency and accuracy of data", EMA TGA and MHRA (Medicines and Healthcare Products Regulatory Agency): "The extent which all data are complete, consistent and accurate throughout data lifecycle". Data manipulations, misrepresentation, tampering, unwarranted deletions / extensions and concealing are serious offence. In the last few years, FDA has issued waring letters and import alert to hundreds of companies in India and abroad. FDA expects that all data generated at the site must pass data integrity criteria as laid down in the official guidelines. It further requires that the data shall be recorded as the job is performed and original / certified copy of the same shall be maintained over its life cycle. FDA has turned very strict about meta-data i.e. date, time, author, subject associated with principle data sets.

The integrity of data is very crucial from FDA point of view. As per many regulatory bodies data integrity is the degree to which re-coded data is complete, consistent and accurate throughout its lifecycle.

According to the United State Food and Drugs Administration (USFDA), 21 CFR part 211.68, 21 CFR part 210, CFR 212 are important regulations to data integrity.

Automatic, mechanical, or electronic equipment or other types of equipment, shall be routinely calibrated, inspected, or checked according to written program design to assure proper performance. Written records of those calibration checks and inspections shall be maintained.

Appropriate controls shall be exercised over computer or related systems to assure those changes in master production and control records or other records are instituted only by authorized personnel and accurate. A backup file of data entered into the computer or related system shall be maintained as a hard copy or alternative systems, such as duplicates, tapes, or microfilm. They should be complete and secure. Such automated equipment used for performance of operations addressed by 211.101 (c) or (d), 211.103, 211.182 or 211.188 (b) (11) can satisfy the requirements include in those sections relating to the performance of an operation by one person and checking by another. (21 CFR part 211.68) [4].

21 CFR PART 11 has guidelines which talk about electronic records and electronic signatures. Electronic records that are required to be maintained under predicate rule requirement and that are maintained in electronic format in place of paper format and also in addition to paper format, and that are relied on to perform regulated activities.

Electronic signature that are intended to be the equivalent of handwritten signatures initials, and other general signings are required by predicate rules. There are a few ways in the approach to specific part 11 requirements. The decision and extent to perform validation of computerized systems are highly necessary.

Audit trail can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation regarding specific part 11 requirements related to computer-generated, time-stamped audit trails. Persons must comply with time or sequencing of events.

Producing copies of records held in common portable formats when records are maintained in these formats. Using established automated conversion or export methods, where available, to make copies in a more common format. Records should be able to be retrieved easily [5].

European Union Annex 11 guidelines apply to all forms of computerized systems used as part of a GMP regulated activities. A computerized system's application should be validated; IT infrastructure should be qualified. Where a computerized system replaces a manual operation, 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. These guidelines are divided into three phases.

The General Phase talks about risk management throughout lifecycle of data. Decisions on the extent of validation and data integrity controls should be based on these documents of risk management of computerized systems. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

The competence and reliability of a supplier, review of documents, quality system and audit information related to suppliers or developers of software and systems should be made available to inspectors. The Project Phase includes validation reports and documentation, ability of change control due to deviations observed during validation process.

An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact.

The Operational Phase talks about Data Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. Risk Management is necessary.

Accuracy checks should be there for critical data entered manually. This check may be done by a second operator or by validated electronic means. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry. Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions which are a system generated "audit trail". For change or deletion of GMP-relevant data the reason should be documented.

Periodic evaluation should be done for computerized systems to confirm that they remain in a valid state and are compliant with GMP. Security is necessary with physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys; pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. Creation, change, and cancellation of access authorizations should be recorded.

Electronic signatures are expected to:

- Have the same impact as hand-written signatures within the boundaries of the company,
- Be permanently linked to their respective record,
- Include the time and date that they were applied. System should allow only qualified persons should certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches through electronic signature.

Archived data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system, then the ability to retrieve the data should be ensured and tested. Pharmaceutical Inspection Convention (PICS)

recently released on August 10, 2016 a detailed 41-page guideline relating to Data Integrity in **Industries, called the Pharmaceutical Inspection Co-Operation Scheme.**

The focus of the document is the Data Governance System where the expectation is that the firm has arrangements for data governance which is documented within their Quality Management System. Such Data Integrity (DI) controls should be risk-based, utilizing the ICH Q9 guidance where any residual Data integrity risk is documented and regularly re-assessed by senior management.

The draft document provides inspectorate guidance on the assessment of Data Criticality and Data Risk when reviewing a firm's Data Integrity Risk Assessment. Referring to the risk management principles described in ICH Q9, the Guidance states: [6].

"The regulated user should perform a risk assessment in order to identify all the GMP/GDP relevant electronic data generated by the computerized systems. Once identified, this critical data should be audited by the regulated user and verified to determine that operations were performed correctly and whether any change (modification, deletion or overwriting) have been made to original information in electronic records. All changes must be duly authorized. The review of data-related audit trails should be part of the routine data review within the approval process."

The Guidance provides further details regarding the roles and responsibilities for data review: "The frequency, roles and responsibilities of audit trails review should be based on a risk assessment according to the GMP/GDP relevant value of the data recorded in the computerized system. For example, for changes of electronic data that can have a direct impact on the quality of the medicinal products, it would be expected to review at each and every time the data is generated" [6].

Therefore, the Guidance is requiring the review of data related audit trails associated with each batch of medicinal product that is produced and tested. The document also discusses Organizational Influences on Data integrity which includes: Code of Ethics; Quality Culture; Quality Metrics and expectations when addressing identified Data Integrity issues. In addition, the document discusses principles of data integrity including the Quality Elements of Data via the ALCOA+ acronym and the specific Data integrity considerations for both paper and computer based systems. It goes on to indicate that firms should establish procedures describing, in detail, both how audit trails are to be reviewed and that the review activity should be documented and recorded. Further, the requirement for investigation of any significant variation detected during the review process and for a procedure that describes the actions to be taken if an audit trail review identifies serious issues that could impact the quality of the medicinal products are also presented. Finally, the Guidance calls for Quality Unit review of a sample of audit trail records during routine self-inspection programs [6].

The data review requirements proposed by the PIC/S Data Integrity Guidance documents are both practical and operational in nature, more so than most other pharmaceutical industry Guidance documents published to date. Use the information gained from these inspections to determine whether revisions to Part 11 or additional guidance on the topic were necessary. FDA also committed to take appropriate enforcement actions on issues identified during the inspections. In the slide deck FDA stresses that they will "continue to enforce all predicate rule requirements, including requirements for records and record keeping. Enforcement actions of FDA in this area continue due to widespread problems.

Figure 3
Paper Requirements = Electronic Requirements

The requirements for record retention and review do not differ depending on the data format;

paper-based and electronic data record-keeping systems are subject to the same requirements.

RESEARCH RESULTS

Investigation procedures include the involvement of other sectors, to find out the cause and background of the intentional data integrity error. Whether it's entirely the personnel's fault or there are other surrounding causes, which might be indirectly due to the management.

Improving Data Integrity in Pharma Industries

Training

Awareness about the company's data integrity policy to the employees and new employees is to be made clear through scheduled training programmers conducted by experienced personnel. To make it easier to understand, it is to be oriented in various languages. This is definitely vital since most of the errors or data integrity issues at the workplace are originated due to humans. These human errors can be drastically prevented by appropriate training and by making the employees believe that these changes do make a huge impact on the quality of the medicines manufactured at the facility. They should understand that the impact of carelessness or fraud will ultimately affect the patients' lives. Training should be given to technical and non-technical operating staff. Data Integrity culture should be followed through data integrity policies and Standard Operating Procedure.

Quality Culture

For maintaining data integrity in the company, the management should make personnel aware of the importance of their role in ensuring data integrity and the implication of their activities to assuring product quality and protecting patient safety. The Standard operating procedure for data integrity should be followed efficiently by all personnel working in the company. A code of value and ethics should be followed and it should reflect the management's philosophy on quality, which is achieved through policies. Management should aim to create a quality culture which is open, one in which personnel are encouraged to freely communicate failures and errors, so that corrective and preventive actions can be taken accordingly. The flow of information between all levels of the organization should be permitted. The collection of values, thought processes and behaviors practiced consistently by management and all personnel contribute to creating a quality culture to assure data integrity.

Computerized Systems

Computer systems should have sufficient controls to prevent unauthorized access or changes to data. There should be a record of any change made as to who made the change and when the change was made. Access to folder deletion software installation and user privileges should be controlled. Computer system validation checks should be done in order to discern invalid or altered records. Computerized systems which exchange data electronically with other systems should include appropriate built in checks for the correct and secure entry and processing of data, in order to minimize risks. A secure location should be allotted for backups of all data in order to prevent intentional or unintentional damage. In case of data review, there has to be regular internal and external audits and verification of the attendance, log books and presence of the person. The frequency of data review should be increased.

Electronic Systems

Biometric signatures are a method to verify an employee's identity based on measurement of an individual's physical features which are unique and measurable to that individual. For example, voice prints, hand prints and retinal scans. These signatures must consist of two distinctive components and must be used by the genuine owner. Ensuring that no two individuals have the same combination of identification codes and that they're periodically checked, recalled or revised is a necessary step in maintaining data integrity within electronic systems.

Better Communication

Communication is a critical element to reduce data integrity challenges within organizations. Workflow simplification and the adoption of industry best practice pre-defined workflows will reduce complexity. With modern tools such as LIMS, ELN, LES the challenge to the industry is to make pairing a balance with a computer using a laboratory software application. Lowering the barrier to integrate instruments will contribute to lowering data integrity challenges in laboratories significantly.

CONCLUSIONS

The objective of this paper was achieved by presenting a strategic and guidance approach to show the importance of maintaining integrity of data parameters in the medical device and pharmaceutical industry throughout the cGMP in a complete manner, consistent and accurate data.

ACKNOWLEDGEMENTS

I want to acknowledge, thank and recognize the support from my family, friends and professors throughout my graduate studies. Special thanks to my project advisor Dr. Edgar Torres for his support and contributions.

REFERENCES

[1] B. W. Unger, "Data Integrity and Data Management for GXP Regulated Firms", Inform. Mar. 2015.

[2] A. Shanley, "Concerns Mount Over Data Integrity and Compliance Issues Abroad", vol. 40, Issue 3 Rep. Mar. 02, 2016.

[3] Z. Brennan, "US FDA Inspections in China: An Analysis of Form 483s from 2015", Newslett., Feb. 10, 2016.

[4] K. Takahashi, "Data Integrity and Compliance with cGMP Guidance for Industry", Develop., Apr. 2016.

[5] U.S. FDA 21 CFR Part 11, "Electronic Records; Electronic Signatures", Inform., Apr. 1, 2017.

[6] J. Davidson, Ph.D., "Follow-up on PIC/S Data Integrity Guidance", Aug. 18, 2016.