Seven Data Integrity Validation Documents and Records Every Life Sciences Executive Needs to Know

Seven Data Integrity Validation Documents and Records Every Life Sciences Executive Needs to Know

Data integrity, which refers to the accuracy and consistency of stored data, is one of the most relevant regulatory topics in quality management today.

It is a crucial issue for pharmaceutical and biotechnology companies that can literally make or break the success of a given product. Properly recorded, reported, and traceable information is essential for offering proof to regulatory investigators that products have been manufactured in line with established protocols, and in assuring products' identity, quality, strength, purity, and safety before market distribution.

This paper will present the seven validation documents and records that every computerized data system should include to be compliant with FDA regulations and international standards. This list represents a practical solution to managing regulatory risk and achieving a sustainable advantage in a marketplace in which this hot-button regulatory issue is becoming ever more prominent.

The Regulatory Framework of Data Integrity

Data integrity is not a new concept for Life Sciences companies, but there are new expectations from regulatory bodies when it comes to data trustworthiness and data quality. The growth and globalization of the industry has put increasing downward pressure on attempts to regulate data integrity.

As recently as April, the FDA issued for comment "Data Integrity and Compliance With CGMP Guidance for Industry," a new draft guidance for the pharmaceutical industry to better explain "the role of data integrity in current good manufacturing practice (cGMP) for drugs."[2] Along with answering frequently asked questions, this draft defined data integrity as "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)."

It also outlined many key requirements from CFR parts 210, 211, and 212 "with respect to data integrity," including:

- 211.68 (requiring that "backup data are exact and complete," and "secure from alteration, inadvertent erasures, or loss");
- 212.110(b) (requiring that data be "stored to prevent deterioration or loss");
- 211.100 and 211.160 (requiring that certain activities be "documented at the time of performance" and that laboratory controls be "scientifically sound");
- 211.180 (requiring that records be retained as "original records," "true copies," or other "accurate reproductions of the original records"); and
- 211.188, 211.194, and 212.60(g) (requiring "complete information," "complete data derived from all tests," "complete record of all data," and "complete records of all tests performed").

The draft correspondingly detailed the key term "audit trail," which it defined as "a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record." Audit trails are crucial concepts to explore in-depth because they are lenses for viewing organizational activity both internally and externally.

It is important to note that each system can have several audit trails that track a specific category of data and activity in categories as diverse as management, operational, security, and technical controls. By providing an accounting of all the information pertaining to a system and its users, audit trails not only collect data for system administrators to review and analyze, but also provide insurance against system failures and legal evidence should protection from compliance issues become necessary.

By providing an accounting of all the information pertaining to a system and its users, audit trails not only collect data for system administrators to review and analyze, but also provide insurance against system failures and legal evidence should protection from compliance issues become necessary.

Depending on the system and protocol, data audit reviews can be done in real-time, periodic, or as necessary. Many tools can be implemented to continually monitor and analyze audit trail data. For example, per the National Institute of Standards and Technology Computer Security Division, this can include adding "preprocessors designed to reduce the volume of audit records to facilitate manual review;" "trends/variance-detection tools [that] look for anomalies in user or system behavior;" and "attack signature-detection tools [that] look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt."[3]

Recent Intensification of Data Integrity Sanctions

As FDA on-site inspections of systems and processes at overseas facilities increase, so has the incidence of data manipulation, document adulteration, and other cGMP infractions in India, China, and other international markets. Data integrity concerns are well-documented in India. Since 2013, the FDA has cited at least 15 companies over the consistency and accuracy of their data. Some of the more serious violations found companies lacked the facility to backup and restore data, allowed laboratory analysts to share Login IDs, and backdated lab data.

In China, FDA inspection teams have discovered circumstances where sample raw data file names were changed, and audit trails disabled. According to Bloomberg, during a recent visit to a pharmaceutical factory in the Chinese city of Taizhou, FDA inspectors noticed that when workers conducted quality tests on drugs for U.S. export, they sometimes didn't record the results, and at other times, deleted them. Some of these violators found themselves placed on an import ban list that prevented them from shipping products to the U.S.

Manufacturers who fail to take satisfactory corrective action may be served with a Form 483, a warning letter, import alert, or other penalty. Examples of firms receiving warning letters for deficient corrections in response to observations in the Form FDA 483 include but are not limited to the following abbreviated citations:

DBA General Devices, Ridgefield, NJ, USA[4]

1. There is a lack of documented software validation for releasing the following Carepoint.exe versions for resolving issues from one customer site.
2. The audio between an iPad and Carepoint EMS WorkStation, Serial No. 0464, was not working. The unit's (b)(4) program was upgraded to version 1.01.26 to resolve the issue. There is a lack of documented software validation for the (b)(4) release.

Sri Krishna Pharmaceuticals Ltd. - Unit II, Andhra Pradesh, India[5]

1. Your firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 211.194(a)).
2. Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records (21 CFR 211.68(b)).

Megafine Pharma Limited, Mumbai, India[6]

1. Failure to ensure that, for each batch of intermediate and API, appropriate laboratory tests are conducted to determine conformance to specifications.
2. Failure to prevent unauthorized access or changes to data and to provide adequate controls to prevent manipulation and omission of data.

Emcure Pharmaceuticals Ltd, Maharashtra, India[7]

1. Your firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 211.194(a)). During our inspection, we observed multiple examples of incomplete, inaccurate, or falsified laboratory records.
2. Furthermore, data falsification and manipulation, and your reliance on incomplete records to release product to the market, are repeat violations. A February 2014 inspection of solid (b)(4) dosage operations at this same facility also reported data manipulation and falsification of test results generated by your firm, along with other deficient laboratory practices that also resulted in products being recalled from the U.S. market.

Responding to violations such as the preceding is time-consuming, and "regulatory actions not only impact the revenue stream of the company, but also affect the drug maker's ability to get approval for new drug applications." [8]

As FDA on-site inspections of systems and processes at overseas facilities increase, so has the incidence of data manipulation, document adulteration, and other cGMP infractions in India, China, and other international markets.

Key Factors in Data Integrity Compliance

Harmful sanctions and negative market consequences can be avoided if data is properly recorded, tracked, managed, and stored in a manner that is easily accessible. In fact, the FDA has regulated automation of the data recordkeeping process via computer systems since 1997.

The first step in meeting data integrity compliance begins with identifying all the requirements within an organization and the various processes in use. The FDA expects any and all systems—be they software or computerized—to have the necessary quality and reliability, and to be working for their designated uses, including intended uses for data integrity.

Of course, it is not enough to have data integrity—you must also be able to prove your data is accurate and your system is secure. The FDA expects you to develop the objective evidence that you have met the data integrity requirements, as well as have the necessary quality and reliability in your systems.

The FDA Standards of Data Quality

At its core, the FDA wants to know how organizations obtained and recorded their data (i.e., prove data quality) and how they collected it properly (i.e., prove data collection process quality).

In terms of meeting their requirements for the collection, oversight, and storage of electronic source data in clinical investigations, the FDA continues to stipulate (as it originally did with paper documents) that the source data should be attributable, legible, contemporaneous, original, and accurate. Known as ALCOA, this list of criteria serves as a guidance structure for proving quality standards in evidence of data quality—as seen previously in the definition of data integrity from the most recent FDA guidance.

Further summarized, good documentation as defined by the ALCOA standards is as such:

- **Attributable:** Knowing where the data came from but also being able to identify the person who entered the data and/or did the work from whence it originated.
- **Legible:** Data is presented in a clear and readable manner. If there are changes to the data, the old values and the new values are both reviewable.
- **Contemporaneous:** Data is entered at the time or as close to possible to when the activity took place.
- **Original:** The earliest record should be included in all data and should not be obscured by subsequent records.
- **Accurate:** Results are a valid representation of the source of data, with the inclusion that all corrections are documented and satisfactory explanations given for why changes occurred.

From data selection and collection to data analysis and reporting, there are many aspects of data integrity that go into compliance with the FDA's ALCOA standards as well as rules and international standards.

How to Achieve Data Validation

With regard to auditing computer systems for data integrity, the key to compliance lies in knowing what to look for in validation documentation. This is important because production process control software must be validated for its intended use according to an established protocol. Furthermore, auditors must be able to identify and review documented evidence of the validation process—including documented evidence of following the process and completing validation tasks—as well as the results of validation activities.

According to the experts at EduQuest and in collaboration with UL, here are the seven critical software and system validation documents and records that should be included with any system:

1. Requirements documents describing the intended use(s) and user needs associated with the software and system.
2. Established validation protocol/plan describing the activities necessary to demonstrate that the requirements can be met.
3. Records of the results of the validation activities described in the validation protocol.
4. Records that show changes are appropriately controlled (where applicable).
5. Records that show appropriate software, system, and quality requirements were established and provided to the vendor, if developed elsewhere. The vendor must be qualified, and the purchasing data and validation results should support that the requirements were met.
6. Records of testing and verification activities, including proper installation.
7. Validation Report that summarizes the activities and documentation as described in the validation protocol/plan, including issues during development and testing.

Building a Culture of Integrity

In order to achieve a lasting organizational commitment to data integrity and validation, leading pharmaceutical and biotech companies are fostering a culture of integrity across their people, processes, and technology. As with almost all organizational and regulatory objectives, the difference between successful or ineffective data integrity management is a direct result of the culture of the organization. Research published in the *Harvard Business Review* pinpoints "four factors that drive quality as a cultural value."[1] They are:

- **Leadership Emphasis:** There must be consistency between executive messaging, action, and the company's mission. Any disconnect causes enthusiasm and commitment to waver which results in lower quality work.
- **Message Credibility:** Management must know what drives quality and committed work and then customize messaging for employees.
- **Peer Involvement:** Companies must clearly define quality initiatives and develop a sense of pride by fostering positive social pressure to create peer engagement that is authentic and self-promoting.
- **Employee Ownership of quality issues:** After giving employees guidance and education, allow employees to take actions that allow them to use their skills and knowledge in creative or corrective decision-making.

Efforts such as establishing digital audit trails and electronic signatures that are compliant with 21 CFR Part 11 and EU Annex 11 will always be core elements in successful data integrity and validation. Leaders in the life sciences will place a premium emphasis on integrating data integrity directly into the business operations and daily considerations of their organization.

Conclusion

Following these criteria will set the foundation for a data integrity program that meets FDA expectations "that data be reliable and accurate."[9] But, as previously noted, document and records validation is just one aspect of ensuring data integrity, and as such, organizations should be prepared to implement meaningful and effective strategies to manage their data integrity risks across the entire spectrum of their operation. This includes isolating database servers and web servers on separate networks; disabling and securing unnecessary network services; instilling and enforcing access controls; recognizing and eliminating known vulnerabilities and exploitations; implementing real-time security warnings; continually monitoring, updating, and auditing systems regularly.

Staying off the regulatory radar and securing organizational data integrity and good documentation practices requires the same thing: a quality approach to manufacturing that encompasses preventing instances of contamination, mix-ups, deviations, failures, and errors in production processes and facilities. According to the FDA's Current Good Manufacturing Practice, this is accomplished by "establishing strong quality management systems, obtaining appropriate quality raw materials, establishing robust operating procedures, detecting and investigating product quality deviations, and maintaining reliable testing laboratories." [10]

For even the most organized and systemized organizations, there are a lot of controls and regulations with which they must comply. That's why companies work with UL to ensure data integrity compliance. With more than 35,000 trained FDA investigators throughout the world and 17 years of partnership with the FDA, UL can educate organizations on best practices, audit management systems, and, should the need arise, UL consulting can guide organizations through the process of FDA inspections, compliance mitigation, and auditing. As part of a new Data Integrity program, which includes eLearning courses written by industry experts, UL is enabling companies to build awareness of the issues and also promote a culture of excellence and improved behaviors.

In the end, whether they seek outside knowledge and expertise or go at it alone, it is the responsibility of companies operating in the life sciences space to implement effective controls and oversight in advance of inspections. Every effort should be made to ensure the accuracy and reliability of data so consumers are protected from buying products that are ineffective or hazardous to their health.

Cited Sources

1. Srinivasan, Ashwin and Kurey, Bryan. “Creating a Culture of Quality.” Harvard Business Review. April 2014.

2. Data Integrity and Compliance With CGMP Guidance for Industry. U.S. Department of Health and Human Services Food and Drug Administration Center for Drug Evaluation and Research (CDER) Center for Biologics Evaluation and Research (CBER) Center for Veterinary Medicine (CVM) April 2016 Pharmaceutical Quality/Manufacturing Standards (CGMP).

3. An Introduction to Computer Security: the NIST Handbook. Doi: 10.6028/NIST.SP.800.12. Chapter Summarization. October 1995.

4. 86 Harriet Ave Corporation DBA General Devices. Public Health Service Food and Drug Administration Warning Letter. 6/1/16.

5. Sri Krishna Pharmaceuticals Ltd. - Unit II. Public Health Service Food and Drug Administration Warning Letter. 4/1/16.

6. Megafine Pharma Limited. Public Health Service Food and Drug Administration Warning Letter. 5/19/16.

7. Emcure Pharmaceuticals Limited. Public Health Service Food and Drug Administration Warning Letter. 3/3/16

8. Analyzing the State of Data Integrity Compliance in the Indian Pharmaceutical Industry, Ernst & Young, 2015.

9. Data Integrity and Compliance With CGMP Guidance for Industry – Draft Guidance, US Food & Drug Administration, April 14, 2016.

10. Facts About the Current Good Manufacturing Practices (CGMPs). http://www.fda.gov/Drugs/DevelopmentApprovalProcess/Manufacturing/ucm169105.htm