astrix

White Paper

Data Integrity in FDA Regulated Laboratories

Data Integrity in FDA Regulated Laboratories

What you need to know

Verification of data integrity is a critical part of the FDA's mission to ensure the safety, efficacy and quality of human and veterinary drugs, biological products, and medical devices. As such, the FDA's expectation is that all data which is submitted to the Agency is both reliable and accurate.

The first indications of data integrity issues in the pharmaceutical industry began in the 1980's, with the revelation that several generic drug manufacturers had submitted fraudulent data to the FDA on their Abbreviated New Drug Applications (ANDAs). Some of these generic drug manufacturers even went so far as to repackage name brand drugs as samples of their own products before submitting them for bioequivalency tests.[1]

While this generic drug scandal put the issue of data integrity on the FDA's radar, it was not until the year 2000 that the FDA issued its first warning letter to a pharmaceutical company for data integrity violations.[2] An abundance of FDA warning letters and form 483 observations related to data integrity issues have been issued in the years since. In 2018 alone, the FDA issued 54 warning letters that had references to data integrity and data management deficiencies in pharmaceutical companies, 10 of which were in the United States. A recent analysis of 2018 warning letters by FDAzilla found that 45% of GMP-related warning letters issued to pharmaceutical companies based in the United States included a data integrity deficiency.[3]

A recent analysis of 2018 warning letters found that 45% of GMP-related warning letters issued to pharmaceutical companies based in the United States included a data integrity deficiency

Enforcement actions by the FDA with respect to data integrity-related cGMP violations can result in serious financial consequences for an organization due to facility shutdown, product recalls, import and/or distribution bans, delayed or denied drug approvals, substantial remediation costs, and loss of customers due to a damaged reputation. Several companies that have been cited for data integrity deficiencies by the FDA over the last 12 years are in fact no longer in business due to the financial hardships that ensued. FDA warning letters also divert worker attention away from their daily activities towards corrective and preventive actions, which can result in significant expenditures of time and money. Additionally, manufacturers who are found in violation of data integrity regulations may lose the trust of the FDA and face more frequent and in-depth inspections in the future.

Citing a "troubling" trend of violations involving data integrity "increasingly" being observed in its cGMP inspections, the FDA published an updated version of its **Data Integrity and Compliance with Drug cGMP** Guidance in December 2018 in an effort to clarify the Agency's current thinking on the creation and handling of data in accordance with cGMP requirements for pharmaceutical manufacturers. In this white paper, we will review this draft guidance and discuss important steps that your organization can take in order to avoid costly data integrity violations moving forward.

What is Data Integrity?

Data integrity is an important consideration in the design, implementation and use of any system that stores, retrieves or processes data. In order to establish data integrity, organizations must take steps to protect original data from accidental or intentional modification, falsification, or deletion and provide assurance that data records are accurate, complete and maintained within their original context. Whether data is recorded in paper or electronic formats, or a hybrid of both, the FDA requires that data be reliable and trustworthy to the extent that it will withstand scrutiny during regulatory inspections.

In its recently released guidance on data integrity, the FDA clarifies that, "For the purposes of this guidance, *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)."

ATTRIBUTABLE

This refers to the fact that a reviewer must be able to determine who collected the data, when it was collected, from which instrument it was collected, and who made any data modifications or manipulations. Note that the use of shared passwords in a LIMS or other informatics system makes it impossible for a reviewer to attribute the data to a specific person.

LEGIBLE

Data must be legible/readable. Electronic data must have the capability to be made readable by humans.

CONTEMPORANEOUS

Data must be recorded at the time it is created, not transcribed at a later date. Data is not transcribed from scrap paper to "official" documents such as laboratory notebooks or batch records.

ORIGINAL

Data must be recorded in the file or format in which it was originally generated (original paper record from a manual observation or electronic raw data file from a computerized system), preserving the accuracy, completeness, content and meaning of the record. The paper printout from an instrument would not be considered official, original GMP data, as it is lacking the necessary complete information – audit trail, metadata, system configuration, etc.

ACCURATE

Recorded data needs to be accurate and 2nd person verified when appropriate. Data that is recorded in multiple locations should be in agreement.

FDA Regulations and Guidance on Data Integrity

Parts 210, 211 and 212 of Title 21 of the Code of Federal Regulations (CFR) contain a number of references to data integrity. Sections §§ 210.1 and 212.2 make clear that cGMP regulations set forth minimum requirements to assure that drugs meet the standards of the FD&C Act regarding safety, identity, strength, quality, and purity. Relevant sections detailing data integrity-related cGMP requirements for pharmaceutical drugs include:

- **§ 211.68:** Backup data should be "exact and complete" and "secure from alteration, inadvertent erasures, or loss" and "input to and output from the computer" should be "checked for accuracy".
- **§ 212.110(b):** All records should be "stored to prevent deterioration or loss, and readily available for review and copying by FDA employees."
- **§§ 211.100 and 211.160:** Production and process control procedures should be "documented at the time of performance" and laboratory controls should be "scientifically sound".
- **§ 211.180:** Records should be retained as "original records or as true copies," or other "accurate reproductions of the original records".
- **§§ 211.188, 211.194, and 212.60(g):** Laboratory records should include "complete information," "complete data derived from all tests," "complete record of all data," and "complete records of all tests performed".
- **§§ 211.22, 211.192, and 211.194(a):** Production and control records should be "reviewed" and laboratory records should be "reviewed for accuracy, completeness, and compliance with established standards".
- **§§ 211.182, 211.186(a), 211.188(b)(11), and 211.194(a)(8):** Records should be "checked," "verified," or "reviewed".

Other regulations which impact data integrity requirements include 21 CFR Part 11, the final rule on Electronic Records and Electronic Signatures, which was released by the FDA in 1997. This regulation defines the criteria in which electronic records and signatures are considered to be trustworthy, reliable and equivalent to paper records. The electronic signature and record keeping requirements specified in 21 CFR Part 11 apply to all FDA-regulated industries, and therefore cover records subject to the requirements set forth in 21 CFR 210, 211 and 212.

The recently released FDA guidance document on data integrity intends to clarify the current good manufacturing practice (cGMP) regulations for drugs with regards to data integrity. Let's take a closer look at this guidance in order to discern the key aspects that impact regulated cGMP laboratories.

Overview of the Recent FDA Guidance Document on Data Integrity

The FDA's **Data Integrity and Compliance with Drug cGMP** guidance document makes it clear that companies need to institute adequate controls and oversight to ensure data integrity. The FDA expects firms to "implement meaningful and effective strategies to manage their data integrity risks based upon their process understanding and knowledge management of technologies and business models." Companies that do not have adequate data integrity controls and oversight in place are considered to be in violation of GMP rules, even if the FDA has not found any instances of actual data deletion, falsification or modification. Warning letters have been issued for simply permitting conditions to exist where data could be changed or deleted. In other words, the FDA is applying a "guilty until proven innocent" approach to data integrity.

The FDA presents a number of questions in this guidance document which may be helpful to ask when considering how to meet data integrity requirements:

- **Are activities documented at the time of performance?**
- **Are controls in place to ensure that data is complete?**
- **Are activities attributable to a specific individual?**
- **Can only authorized individuals make changes to records?**
- **Is there a record of changes to data?**
- **Are records reviewed for accuracy, completeness, and compliance with established standards?**
- **Are data maintained securely from data creation through disposition after the record's retention period?**

Some of the key parts of this guidance document that impact regulated cGMP laboratories include:

1. Risk-Based Data Integrity Strategy

This new guidance emphasizes the importance of creating a flexible and risk-based company-wide data integrity strategy, and strongly suggests that management should be involved with both the development and implementation of this strategy. Effective strategies "should consider the design, operation, and monitoring of systems and controls based on risk to patient, process, and product."

2. Metadata

Metadata is data that provides information about other data and is necessary to reconstruct cGMP records. As such, metadata "describes, explains, or otherwise makes it easier to retrieve, use, or manage data." The FDA expects that "data should be maintained throughout the record's retention period with all associated metadata required to reconstruct the CGMP activity."

3. Audit Trails

Audit trails and their reviews are an important requirement in current cGMP regulations. As defined by the guidance, an audit trail is "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 important to the FDA, as they ensure the trustworthiness of the electronic record, demonstrate necessary data ownership, and assure records have not been modified or deleted.

The FDA considers audit trails to be part of an associated record and recommends that "Personnel responsible for record review under cGMP should review the audit trails that capture changes to data associated with the record as they review the rest of the record." Audit trail review frequency should adhere to data/record review frequency specified in cGMP regulations. For example, 21 CFR Part 211.22 requires data review before batch release.

If the review frequency for the record is not specified in CGMP regulations, you should determine the review frequency for the audit trail using knowledge of your processes and a risk assessment that includes evaluation of data criticality, control mechanisms, and impact on product quality.

4. Access to Computerized Systems

The FDA recommends that companies maintain computer system access controls in order to assure that changes to records can only be made by authorized personnel. Amongst other things, this means that each person accessing the computerized system must be able to be uniquely identified, and their actions within the system should be trackable via an audit trail. Additionally, rights to alter files and settings (e.g., system administrator role) in the computer system should not be assigned to those responsible for record content – small companies are no longer excluded from this requirement.

5. Control of Blank Forms

As uncontrolled blank forms (e.g., worksheets, laboratory notebooks, master production and control record, etc.) provide an opportunity for falsifying data and/or "testing into compliance," the FDA recommends that all blank forms be uniquely numbered and tracked. Electronic workflows allow this process to be automated – a clear advantage over paper-based systems.

6. GMP Records

The FDA states that, "When generated to satisfy a GMP requirement, all data become a GMP record." As such, the "FDA expects processes to be designed so that data required to be created and maintained cannot be modified without a record of the modification." This means that "it is not acceptable to store electronic records in a manner that allows for manipulation without creating a permanent record." Additionally, it is not acceptable to record data on a sticky note that will be discarded after the data are transcribed to a permanent laboratory notebook – the original record containing the data must be stored securely throughout the record retention period.

7. System Suitability Testing

The FDA considers it a regulatory violation to use actual samples in system suitability test, prep, or equilibration runs as a means of disguising "testing into compliance." In this guidance, the FDA has clarified its thinking regarding the use of actual samples during system suitability testing. Such samples should be a properly characterized secondary standard from a different batch than sample(s) being tested. cGMP records must provide transparency and be complete. "All data – including obvious errors and failing, passing, and suspect data – must be in the CGMP record."

8. Computer System Validation (CSV)

In this new guidance, the FDA has expanded its discussion of CSV to emphasize that validation studies on computer systems "should be commensurate with the risk posed by the automated system" and should validate the system for its intended use. Validating the system for intended use ensures that the intended steps, specifications, and calculations involved in a workflow are accurate. The FDA recommends that you implement controls to manage risks associated with each aspect of the computerized workflow - software, hardware, personnel, and documentation. The clear implication is that computer system validation should not be isolated within the IT department but should instead be connected with the company quality unit.

The 2018 guidance states that, in addition to receiving training in detecting data integrity issues, personnel must be training in preventing data integrity issues.

9. Employee Training

The 2018 guidance states that, in addition to receiving training in detecting data integrity issues, personnel must be training in preventing data integrity issues. The FDA wants firms to train their personnel to develop corrective and preventative actions so that data integrity issues are mitigated and do not recur.

10. Backup Records

The FDA clarifies that the term "backup" refers to "a true copy of the original record that is maintained securely throughout the record retention period." Additionally, "backup data must be exact, complete, and secure from alteration, inadvertent erasures, or loss."

11. Shared Logins

The FDA requires unique logins for all users that have permission to modify data. However, shared login accounts for users accessing the system for read-only data viewing are acceptable. Be aware, however, that these shared login accounts do not "conform with the part 211 and 212 requirements for actions, such as second person review, to be attributable to a specific individual."

12. FDA Access to Records

The FDA clarifies that it can review "records generated and maintained on computerized systems, including electronic communications that support cGMP activities." Relevant email communications (e.g., email to authorize batch release) can be reviewed, for example.

13. Electronic Copies

The FDA states that "Electronic copies can be used as true copies (backup of the original) of paper or electronic records, provided the copies preserve the content and meaning of the original data, which includes associated metadata and the static or dynamic nature of the original records."

14. Addressing Data Integrity Violations

Regardless of how a data integrity violation is discovered (e.g., third party audit, FDA audit, internal tip, etc.), the new guidance makes it clear that all identified data integrity errors "must be fully investigated under the cGMP quality system to determine the effect of the event on patient safety, product quality, and data reliability." The investigation should determine the root cause and ensure the necessary corrective actions are taken. Necessary corrective actions may include hiring a third-party auditor, removing individuals responsible from cGMP positions, improvements in quality oversight, enhanced computer systems, creation of mechanisms to prevent recurrences, etc.

Implementing a Data Integrity Strategy

Data management that ensures both the security and reliability of data must be effectively incorporated into your organization's Quality Management System. As regulatory focus on data integrity is showing no signs of abating, manufacturers would be wise to implement a risk-based strategy to meet cGMP regulations on data integrity. Recommended aspects of this strategy include:

Make Sure That QC and IT Departments are Working Together:

Validating individual computer systems is often not enough to ensure data integrity across the full data lifecycle, which can span many different systems and even extend out to CROs, CMOs, partners, suppliers, etc. The Quality Control unit should be in active partnership with the IT department in order to implement the Quality Management System and create a culture of compliance that ensures data integrity issues are addressed in computer systems and SOPs across the enterprise.

Perform a Risk Assessment and GAP Analysis:

It is essential to perform a GAP Analysis on your organization's processes and systems with regards to data integrity regulations. This should be accompanied by a determination of the risk associated with each process or system and the data which is generated or modified by it. The level of risk associated with a process or system should be a key consideration when deciding whether to implement/modify technical or procedural controls. Once implemented, reviews of systems, controls and data should occur at a frequency consistent with the level of risk present, the type of system and regulatory requirements.

Foster Company-Wide Data Integrity Awareness:

Training for all employees should strive to create awareness of the concept of data integrity and its importance, as every employee of the company has a direct or supportive role to play in documentation of laboratory results and other records required by GxP rules. This will help establish a company-wide culture of compliance. Data integrity training should highlight the parts of an employee's job that potentially contribute to or create data integrity violations. This is especially important for laboratory staff in order to reduce the tendency to cut corners.

Adopt an Informatics Infrastructure That Supports Data Integrity Regulations:

The FDA realizes that it cannot always trust hard copy paper data records that are provided to them during an inspection. With the release of the 21 CFR Part 11 regulation and its latest guidance on data integrity, the FDA is clearly encouraging the use of laboratory informatics systems that can provide technical controls over data management. Towards this end, it is important to implement a laboratory informatics system from a vendor that stays up to date on current FDA regulations and guidance and has designed their software to support compliance with current FDA recommendations on data integrity and management. Some basic items to look for in a data integrity-oriented laboratory informatics system include:

- **Configurable workflows**
- **User permissions designation and user rights administration**
- **Unique passwords for all users**
- **Password policies – length and character mandates, failed attempts lockout, password expiration and reuse restrictions**
- **User access records – a list of all users and associated permissions**
- **Data security tools**
- **Audit trails with ability to track all necessary components required by regulations from result all the way back to raw data**
- **Access to a clock in order to provide time stamps of who accessed data and how data was edited and imported**
- **Record management**
- **Document revision controls**
- **21 CFR Part 11 compliant electronic signatures**

Consider Data Integrity Issues When Upgrading Legacy Laboratory Informatics Systems:

Data migrations and upgrades to legacy systems must be done with an eye towards data integrity. It is important to note that recent FDA regulatory inspections have examined the migration to new informatics systems to ensure that data and audit trails have transferred over correctly.

Create Audit Trail Review SOPs:

All electronic data, including audit trails, should be reviewed for accuracy as part of laboratory result verification, out of specification (OOS) result investigations, or lot release. An accurate audit trail is important to the FDA, as it allows reviewers to determine whether data has been altered or deleted, which is of particular interest for OOS results. The bottom line is: How quickly can data audit trails be shown to a regulatory inspector? If it takes your staff a long time to locate an audit trail, it suggests that they are not being regularly reviewed.

Utilizing a quality external consultant with expertise in data integrity evaluations for your GMP audit is best practice.

Qualify Instruments:

Establishing data integrity across the full data lifecycle includes ensuring data sources are reliable and accurate. In order to assure data integrity from analytical instruments in the laboratory, these instruments need to be qualified to show they are working properly before any analytical methods are developed or validated using them.

Maintain Data Backup and Recovery Procedures:

A data backup and recovery strategy is necessary in the case of unexpected data loss and/or application error. This creates a safeguard to protect the integrity of your records.

Conduct Regular Audits of Data Integrity:

Firms should include data integrity assessments in GMP audit programs. Audits may be conducted by internal staff in the Quality unit, or by an independent third party. If audit functions are outsourced to an external consultant, be sure to verify that auditors have appropriate training in data integrity evaluations. Utilizing a quality external consultant with expertise in data integrity evaluations for your GMP audit is best practice, as an expert with fresh eyes will likely be able to locate any data integrity issues you missed. The periodic review results, along with any gaps and corresponding remediation activities, must be documented.

Conclusion

Data integrity is a primary focus of the FDA and will continue to be so until the pharmaceutical industry takes meaningful corrective actions to address shortcomings in this area. For the time being, regulators continue to identify the same set of data integrity violations industry-wide, some of which include: shared passwords, failure to review electronic data and audit trails, failure to contemporaneously record data, lack of audit trails, failure to adequately investigate OOS test results, etc.

While the Quality Control laboratory is the most frequent area to identify data integrity issues, data management concerns span the entire enterprise and pharmaceutical product lifecycle. Data integrity audits have almost always focused on Quality Control laboratory records in the past, but the intensive focus on data integrity is beginning to change this. R&D laboratories, clinical research efforts and batch records in production are also starting to come under regulatory data integrity scrutiny.

The bottom line is that requirements for data integrity are not going away. Given that remediation of FDA data integrity enforcement actions tends to be significantly more expensive than finding and correcting issues internally, it is wise to have an effective Quality Management System in place to identify and correct data integrity deficiencies without the need for intervention by the FDA.

Additionally, companies should consider that data integrity requirements apply across the GxP spectrum and are not limited to GMP activities alone. Ultimately, whether your organization is a drug manufacturer, clinical research organization (CRO) or pharmaceutical R&D company, data integrity is a critical issue that is necessary to ensure the safety and efficacy of the life-saving medications that you are a part of producing.

[1] "Generic Drug Price Scandal: Too Bitter a Pill for the Drug Price Competition and Patent Term Restoration Act to Swallow," Notre Dame Law Review, Volume 75, Issue 1, October 1st, 1999. Joseph P. Reid. Available at: http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1579&context=ndlr

[2] Warning Letter to Schein Pharmaceuticals available at: http://www.ofnisystems.com/Resources/Warning_Letters/m3450n.pdf

[3] "Part 2: An Analysis of FDA FY2018 Drug GMP Warning Letters," FDAzilla, March 2019. Barbara Unger. Available at: https://blog.fdazilla.com/2019/03/pharma-part-2-an-analysis-of-fda-fy-2018-drug-gmp-warning-letters/

[4] "Data Integrity: The Whole Story," FDAzilla, April 2015. Barbara Unger. Available at: http://blog.fdazilla.com/2015/04/data-integrity-the-whole-story/

[5] "Data Integrity and Compliance With Drug cGMP: Guidance for Industry," U.S. Department of Health and Human Services, FDA, December 2018. Available at: http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM495891.pdf

[6] Available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=3ee286332416f26a91d9e6d786a604ab&mc=true&tpl=/ecfrbrowse/Title21/21tab_02.tpl

[7] Available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=2949d48976fa732a1280941faf15e154&mc=true&tpl=/ecfrbrowse/Title21/21cfr11_main_02.tpl

About Astrix

Astrix Technology Group is a full-service global laboratory informatics consulting, regulatory advisory and professional staffing firm focused on serving the scientific community since 1995. Our experienced professionals help organizations implement innovative informatics solutions that turn data into knowledge, increase organizational efficiency, improve quality and facilitate regulatory compliance. If you have any questions about Astrix Technology Group offerings, or would like have an initial consultation with someone to explore how to reduce your compliance risk around data integrity, please contact us at **www.astrixinc.com** for a free, no obligations consultation.