astrix
TECHNOLOGY GROUP

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]

A recent analysis of 2016 warning letters by the FDAzilla Newsletter found that 80% of GMP-related warning letters issued to pharmaceutical companies based in the United States included a data integrity deficiency.

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 2016 alone, the FDA issued 41 warning letters for data integrity and data governance deficiencies in pharmaceutical companies, 7 of which were in the United States.[3] A recent analysis of 2016 warning letters by the FDAzilla Newsletter found that 80% of GMP-related warning letters issued to pharmaceutical companies based in the United States included a data integrity deficiency.[4]

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. 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. 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.[5]

Citing a "troubling" trend of violations involving data integrity "increasingly" being observed in its cGMP inspections, the FDA published a draft guidance document entitled "Data Integrity and Compliance With cGMP" in April of 2016 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 provides assurance that data records are accurate, complete and maintained within their original context. In order to establish data integrity, organizations must take steps to protect original data from accidental or intentional modification, falsification, or deletion. 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 draft 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. Specifically, the following sections contain information regarding data integrity-related cGMP requirements for pharmaceutical drugs, among other things: Parts 210.1, 211.68, 211.100, 211.160, 211.180, 211.188, 211.194, 212.2, 212.60, 212.110.

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 recent FDA guidance document released in April of 2016 – Data Integrity and Compliance With cGMP – 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 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.

This guidance document is organized in question and answer format, and is specifically focused on the interpretation of aspects of the regulations for cGMP (21 CFR 11, 210, 211 and 212) that pertain to data integrity issues in a pharmaceutical manufacturing environment. The main purpose of the guidance seems to provide clear and concise solutions to common issues in an easy to follow Q&A format.

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

1. 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." Examples of metadata include: date/time stamp indicating when the data was gathered, user ID of the person that generated the data, ID of the device or instrument used to acquire the data, information useful in interpreting the data, audit trails, etc. The FDA expects that "data should be maintained throughout the record's retention period with all associated metadata required to reconstruct the CGMP activity."

2. Audit Trails

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. An audit trail is a chronology of the "who, what, when, and why" of a record." The FDA considers audit trails to be part of an associated record, and recommends that "audit trails that capture changes to critical data be reviewed with each record and before final approval of the record." Audit trails that capture changes to data should be reviewed by the same personnel responsible for record review under cGMP.

3. Computer Workflow Validation

The FDA recommends that you not only validate computer systems, but also validate them for their intended use or workflow. 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.

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. Ideally, personnel with rights to alter files or settings (e.g., system administrator) should be different from those responsible for record content.

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." All GMP records must be evaluated by the quality unit as part of release criteria, unless there is a valid, documented, scientific justification for its exclusion. Additionally, "The FDA expects processes to be designed so that quality data that is required to be created and maintained cannot be modified." This means that the original record containing the data must be stored securely throughout the record retention period.

7. Use of Samples for "System Suitability" or Test, Prep, or Equilibration Runs

In order to avoid the practice of "testing into compliance," the FDA recommends the use of replicate injections of a standard preparation or other standard solutions using actual product samples for system suitability tests. In the case where an actual product sample is used to perform a system suitability test, "it should be a properly characterized secondary standard, written procedures should be established and followed, and the sample should be from a different batch than the sample(s) being tested."

8. Dynamic and Static Records

The FDA explains that, "For the purposes of this guidance, static is used to indicate a fixed-data document, such as a paper record or an electronic image, and dynamic means that the record format allows interaction between the user and the record content." Electronic records from certain types of laboratory instruments are dynamic records, in that they can be modified by an analyst. Original copies of records, whether static or dynamic:

- should be subject to second-person review to make certain that all test results are appropriately reported
- should be complete and include all appropriate metadata
- must be securely maintained throughout the record retention period.

9. 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."

10. Electronic Signatures

When appropriate controls are in place, electronic signatures can be used in place of handwritten signatures in any cGMP required record. Companies using electronic signatures should document the controls used to ensure that they are able to identify the specific person who signed the records electronically and securely link the signature with the associated record.

11. Data Integrity Training

The FDA states that all personnel should be trained in detecting and avoiding data integrity violations as part of a routine CGMP training program.

12. Tips Regarding Data Integrity Violations

Any suspected falsification or alteration of cGMP records must be fully and formally investigated and documented under the cGMP quality system. The investigation should:

- determine the root cause
- determine the effects on patient safety, product quality, and data reliability
- ensure the necessary corrective actions are taken

13. Addressing Data Integrity Issues Identified During an Inspection

The FDA recommends taking the following actions to demonstrate that you have addressed data integrity issues that were identified during an inspection:

- hire a third-party auditor
- determine the scope of the problem
- implement an enterprise-wide corrective and preventive action (CAPA) plan
- remove individuals responsible for any problems from cGMP positions at all levels.

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:

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.

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.

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. 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. Computerized systems selected by labs need to be qualified to ensure that data integrity is preserved. 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**

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.

Qualify Instruments

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.

Validate Computer Systems

All computer systems should be identified and periodically validated for intended use, and the validation process should be documented. Computer systems requiring validation include laboratory informatics systems, laboratory instrument associated computer systems, and any computerized controls applied in manufacturing equipment. On a practical note, laboratory instrument associated computer systems cannot be validated until the analytical instrument is qualified.

Make Sure That QC and IT Departments are Working Together

Computer system validation and lifecycle management should not be solely the responsibility of the IT department. Instead, this function should be shared with the Quality unit and other stakeholders. The Quality Control unit should be in active partnership with the IT department in order to that ensure that data integrity issues are addressed in computer systems. The Quality unit staff may need additional training to be able to provide effective review of computer system processes and procedures.

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.

ENDNOTES

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 "Warning Letters 2016 – Data Governance & Data Integrity," FDAzilla, May 2017. Barbara Unger. Available at: http://blog.fdazilla.com/2017/05/warning-letters-2016/

4 "Warning Letters 2016 – Data Governance & Data Integrity," FDAzilla, May 2017. Available at: http://blog.fdazilla.com/2017/05/when-will-the-fda-move-on-from-data-integrity/

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