What the FDA Guidance on Data Integrity Means for Your Lab

Regulatory agencies worldwide are increasingly focusing their efforts on data integrity in GxP laboratories. This increased focus has led to a number of guidance documents being published on data integrity in 2016, including:

- The World Health Organization (WHO) published its final version of "Good Data and Records Management Practices" guidance document
- The European Medicines Agency (EMA) issued good manufacturing practice (GMP) guidance to ensure the integrity of data
- The Food and Drug Administration (FDA) issued a "Data Integrity and Compliance With cGMP" guidance document

In its "Data Integrity and Compliance with cGMP" guidance document, the FDA cites a "troubling" trend of violations involving data integrity "increasingly" being observed in its cGMP inspections. A recent analysis by PricewaterhouseCoopers' Health Research Institute (HRI) shows that a growing number of pharmaceutical companies have been warned by the FDA for data integrity violations since 2010 - from 2010 to 2012, the FDA warned five companies for such violations; between 2013 and 2015, the number was 24. The issue has been particularly troubling for offshore API manufacturers. According to a recent article published in BioProcess International, since May 2013 the FDA has issued warning letters to more than 10 big Indian pharmaceutical companies (including Sun, USV Ltd., Wockhsrdt Ltd., and RPG Life Sciences Ltd.) over problems with data integrity. These issues typically revolve around not reporting failed results, conducting unofficial analyses, deleting electronic data, disabling audit trails in electronic data capture systems, fabricating training records, reanalyzing failed samples until passing results are obtained, back- dating data, and not reporting stability failures.

Given that the FDA is clearly concerned about data integrity and intends to enforce cGMP rules related to this topic, how can you be sure that your operations are aligned with the FDA's current thinking on data integrity?

Data Integrity and Why It's Important

Data integrity is the maintenance and assurance of the accuracy and consistency of data over its entire life-cycle. With regards to pharmaceutical manufacturing, the FDA expects that all data submitted to the agency in an effort to gain drug approval is complete, consistent and accurate. Data integrity is a fundamental principle in pharmaceutical manufacturing that enables traceability of a batch back to its origin and thereby ensures that drugs are made and tested according to required quality standards.

From the perspective of regulatory agencies, data integrity violations arise from poor systematic control of data management systems. Lack of proper controls can result in data errors due to human error, a lack of knowledge, or from intentionally hidden, falsified or misleading data. The three most common data integrity issues cited by FDA for inspections from 2013 to 2015 were the lack of controls to prevent alterations of data by staff, failure to maintain records of accurate data, and delayed reporting of data. Data integrity violations can result in financial loss for pharmaceutical companies due to facility shutdown, product recalls, import bans, and delayed or denied drug approvals. Additionally, FDA warning letters divert worker attention away from their daily activities towards corrective and preventive actions, which can cost significant time and money. These violations can also tarnish the company's reputation and provide competitors with an opportunity to increase their market share.

Overview of the FDA Guidance

The FDA's "Data Integrity and Compliance with cGMP" 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* 211) that pertain to data integrity issues in a pharmaceutical manufacturing environment. The 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 or manipulation. In other words, the FDA is applying a "guilty until proven innocent" approach to data integrity.

The main purpose of the guidance seems to provide clear and concise solutions to common issues in an easy to follow Q&A format. It starts with key definitions and then goes on to address critical issues such as inclusion or exclusion of data from decision making process, access control, validation of data, good documentation practices, audit trails, electronic and paper raw data, training, ways to handle data falsification, and scope of an FDA audit of data. Each issue is explained with specific examples and provides clear instructions on FDA's expectations.

So, what are some of the key aspects of the FDA's guidance document that impact regulated cGMP laboratories?

1. **ALCOA:** Companies should establish Data Integrity controls to ensure that data are **A**ttributable, **L**egible, **C**ontemporaneously recorded, **O**riginal or a true copy, and **A**ccurate. The "contemporaneously recorded" stipulation means that data must be documented and saved to storage *at the time it is created*. It is not acceptable, for example, for an analyst to record data on a piece of paper and later transcribe this information to a controlled laboratory notebook.
2. **Metadata and Audit Trails:** Metadata is information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. Metadata could be a date/time stamp describing when the data was acquired, a user ID of the person who conducted the test that generated the data, the instrument ID used to acquire 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.

3. **Audit Trail Review:** The FDA recommends that "audit trails that capture changes to critical data be reviewed with each record and before final approval of the record."
4. **Computer Workflow Validation:** The FDA recommends that you not only validate computer systems, but also validate them for their intended use or workflow. 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.
5. **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 uniquely identified and their actions within the system tracked and audit trailed. Additionally, the FDA recommends that companies "restrict the ability to alter specifications, process parameters, or manufacturing or testing methods by technical means where possible."
6. **Control of Blank Forms:** As uncontrolled blank forms present an opportunity for data falsification 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.
7. **GMP Records:** The FDA states that, "When generated to satisfy a GMP requirement, all data become a GMP record." This means that the original record containing the data must be stored securely throughout the record retention period. Additionally, "The FDA expects processes to be designed so that quality data that is required to be created and maintained cannot be modified."
8. **Dynamic vs. 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, must be securely maintained throughout the record retention period.
9. **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.

Conclusion

While a recent increase in data integrity violations has prompted the FDA's increased focus in this area, the majority of non-compliance citations in routine inspections result from poor systems rather than intentional fraudulent activity. Many companies simply fail to employ robust systems with built-in features that inhibit data integrity failures. When developing data integrity practices for a cGMP environment, many companies make the mistake of relying on the saying "If it's not documented, it didn't happen" in order to guide their work. To reflect the FDA's current thinking on the matter, however, this statement should be adjusted to read: "If it's not documented *completely, consistently, and accurately*, it didn't happen."

The implications of the FDA's recently released guidance document on data integrity are clear – the FDA takes both good documentation practice and data integrity seriously, and intends to enforce cGMP regulations with a "guilty until proven innocent" approach. It is therefore critical for companies to implement robust systems with effective data integrity controls and oversight in order to avoid unpleasant financial consequences from enforcement actions.

About the Author

Dale Curtis Jr. is the President of Astrix Technology Group. For over 18 years, Mr. Curtis has built an impressive track record of leadership and success in high technology/scientific enterprise software sales, business development and service delivery. He has proven talent for driving innovative operational and marketing strategies, building successful teams, and rapidly developing new markets for start-up companies as well as multimillion-dollar global technology enterprises. Mr. Curtis holds a B.S. in Chemical Engineering from the University of Virginia and an M.B.A. from the Drexel University LeBow College of Business.

About Astrix Technology Group

Scientific resources and technology solutions delivered on demand

Astrix Technology Group is an informatics consulting, professional services and staffing company dedicated to servicing the scientific community for over 20 years. We shape our clients' future, combining deep scientific insight with the understanding of how technology and people will impact the scientific industries. Our focus on issues related to value engineered solutions, on demand resource and domain requirements, flexible and scalable operating and business models helps our clients find future value and growth in scientific domains. Whether focused on strategies for Laboratories, IT or Staffing, Astrix has the people, skills and experience to effectively shape client value. We offer highly objective points of view on Enterprise Informatics, Laboratory Operations, Healthcare IT and Scientific Staffing with an emphasis on business and technology, leveraging our deep industry experience.

For More Information

For more information, contact Dale Curtis, President at Astrix Technology Group, dcurtis@astrixinc.com or visit our website at www.astrixtechgroup.com.