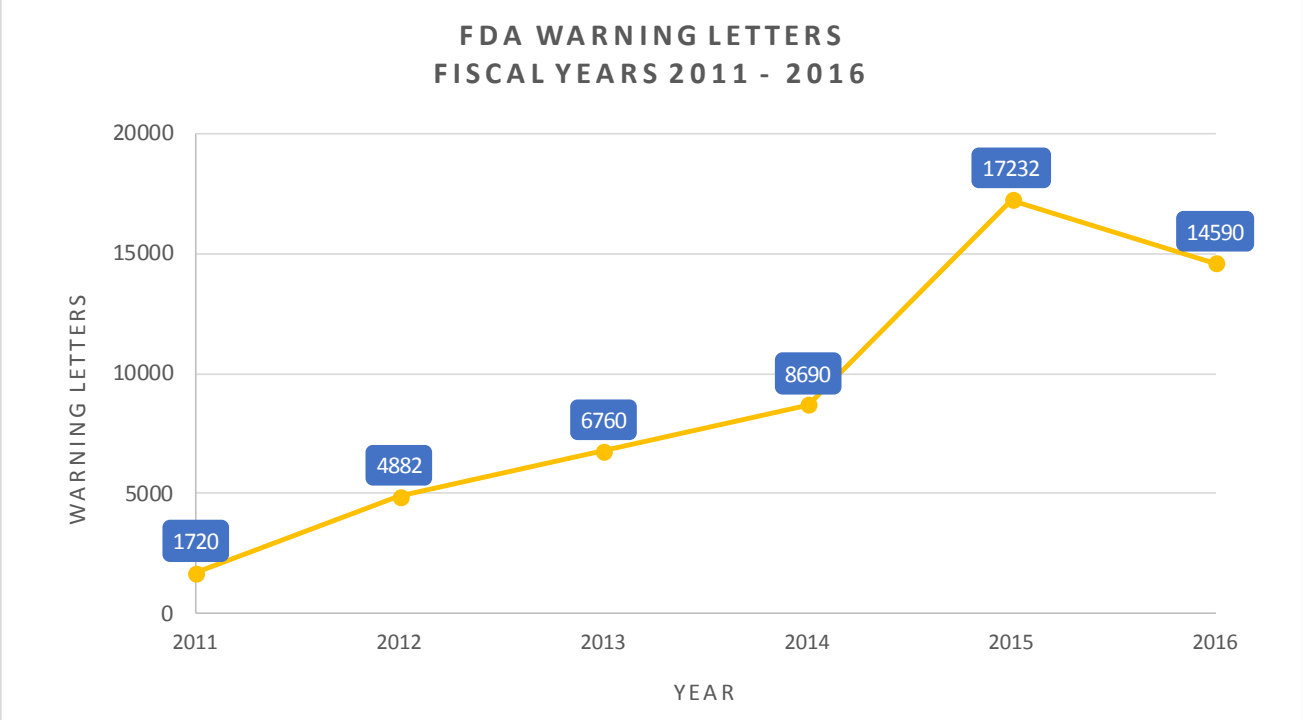
Data Integrity: Understanding and Becoming Compliant with GMP and FDA Requirements

Introduction

Data integrity means data (such as from personnel or environmental monitoring) that is accurate, complete and repeatable, which in turn ensures the product's quality and public safety. In recent years, infractions relating to data integrity have been noted in several Food and Drug Administration (FDA) warning letters, but it is not a new concept. The importance of record-keeping in drug manufacturing can be seen as far back as 1938, when the Federal Food, Drug, and Cosmetic (FDC) Act required the safety of new drugs be documented before being sold to the public, with similar regulations instigated in Europe and Japan throughout the 20th century[1].

Production systems have large, inherent operational risks and are difficult to validate. Instead of only being reactive to public health disasters, preventative measures, such as the requirement for proof of claims, are taken to lower their likelihood and propagate confidence in manufacturers.



Worldwide, data integrity issues (such as manipulation) were the reason for more than one-third of all regulatory actions in 2016.[2]

Warning letters related to data integrity issues more than doubled from 2015 to 2016.[3]

Presence in Regulations

In the past few years, several FDA warning letters (483s) have been issued for data integrity deficiencies in the pharmaceutical industry. In 2016, more than 50% of MHRA warning letters involved data integrity lapses for computerized systems compared to the previous year.[4] Inspectors are actively trained in data integrity requirements, and strongly enforce them for falsified batch records or discharging of raw data.

Understanding recent standards, guides and regulations pertaining to data integrity is essential to becoming compliant. Relevant documents include 21 CFR Part 11, MHRA: GxP, EU GMP Annex 1, the FDA Data Integrity and Compliance with cGMP, and the WHO Good Data and Record Management Practices. Inherent to data integrity compliance is the goal of increasing product quality, regulator confidence, brand reputation and process control while reducing product defects and costs. This applies to multiple areas of the pharmaceutical industry, including manufacturers of finished drug products for clinical trials, bioequivalence studies and commercial distribution, laboratories, contract manufacturing, suppliers etc.

21 CFR Part 11

Title 21 of the FDA's Code of Federal Regulations (CFR) Part 11[5] is the most widely used standard for appropriate data management. Part 11 applies to records in electronic format that are created, modified, maintained, archived, retrieved or transmitted according to requirements set in FDA regulations. Electronic records/signatures that meet Part 11 requirements may be used in lieu of paper records.

The document is divided into three parts:

- General Provisions
- Electronic Records
- Electronic Signatures

GENERAL PROVISIONS

Terms

The General Provisions section gives an overview of the terminology used throughout the document and the types of records that apply and do not apply. The following are essential terms to be familiar with:

Electronic records include text, graphics, data, audio, pictorial, or other information in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. These records must contain data and metadata in a legible format. In addition, they must be ready to retrieve during the entire period of retention.

SIGNED ELECTRONIC RECORDS SHALL CONTAIN:

- **SIGNER'S PRINTED NAME**
- **DATE AND TIME** when the signature was executed
- **SIGNATURE'S MEANING** (such as review, approval, responsibility, or authorship)

A **digital signature** is an electronic signature based on cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

An **audit trail** is a documented, chronological record of system activities with details of how the activities have affected a specific operation, procedure, or event.[6] The audit trail is comprised of records that are secure, computer-generated and time-stamped, and contains the who, what, when and why of the record.
The FDA recommends a review of audit trails that capture changes to critical data alongside each record before final approval of the record.

> The audit trail shall be computer-generated and time-stamped.
>
> It must record the date and time of operator entries and action that create, modify or delete an electronic record.
>
> - 21 CFR PART 11

ELECTRONIC RECORDS — System Validation

Computerized systems must be validated to ensure data accuracy, reliability and consistency, and must be able to discern invalid or altered records. They also must generate an accurate, complete and human-readable copy of the records. Access must be limited with the use of an ID and password.

Those who develop, maintain, or use electronic record/electronic signature systems must have the education, training, and experience to perform their assigned tasks, which is essential to guarantee data integrity.

ELECTRONIC SIGNATURES — Identification Control with ID and Password

Users who intend to generate electronically/digitally signed records must have a controllable form of identification. This control extends to maintaining a unique password and ID code (username), periodic password checks/changes, and configuration of individual and/or group ID privileges (i.e. differentiation between operator, supervisor and administrator). For example, it should not be possible for operators to have database management rights.

ALCOA

ALCOA is an acronym used by the FDA that stands for Attributable, Legible, Contemporaneous, Original, and Accurate.[7] The concept behind ALCOA is that data quality directly impacts product quality, with focus placed on performing tasks correctly the first time and immediate reporting of results. As ALCOA is used in many FDA regulatory documents, it is important to be familiar with what is meant by each term.

ATTRIBUTABLE	LEGIBLE	CONTEMPORANEOUS	ORIGINAL	ACCURATE
Who acquired the data and when was the action performed?	*Is the data able to be read by others for the full duration of the retention period?*	*Is the data documented at the time of the activity?*	*Is the raw data or source data available in its original form/is there a true copy?*	*Does the data contain context/ meaning (i.e. metadata)?*

WHAT IS METADATA?

Metadata is an explanation of the data it refers to. As an example, say you are given a data value of "300". The metadata is what gives this value context, which is that it is the counts per cubic meter for a particle counter.

EU GMP Annex 11

As part of the European Union (EU), EudraLex is the collection of rules and regulations governing medicinal products (for human and veterinary use). Annex 11[8] is part of the European GMP Guidelines and contains terms of reference for computerized systems used by organizations in the pharmaceutical industry. Note that Annex 11 is a guidance, not a regulation (21 CFR Part 11 is a regulation).

Annex 11 defines the criteria for managing electronic records and signatures. These guidelines are similar to those of their US counterpart. The central consideration of both the EU GMP Annex 11 and 21 CFR Part 11 documents is to ensure that records are entered correctly, cannot be tampered with, can be stored for the retention period as well as retrieved (in full) at any time during use and during the retention period. In each regulation, there is a strong focus on record accuracy, integrity, security and retrieval.

From the guidance, there are several important components of a proper data management system, which forms the basis for the following recommended standard operating procedures (SOPs):

SYSTEM MAINTENANCE SOP	Appropriate maintenance must be carried out in a controlled way.
PHYSICAL SECURITY SOP	There must be controls in place that ensure secure access and prevent intrusion.

LOGICAL SECURITY SOP	There must be a user and password policy.
INCIDENT AND PROBLEM MANAGEMENT SOP	There must be a way to manage and communicate a possible problem.
SYSTEM CHANGE CONTROL SOP	It must be understood how any changes may affect the process.
DISASTER RECOVERY SOP	There must be a way to ensure data is protected and the process is recoverable in a disaster scenario.
BACKUP AND RESTORATION SOP	Regular data backup must be controllable.

FDA Data Integrity and Compliance with cGMP Guidance for Industry

This FDA guidance document is currently a draft guidance[9] intended to clarify the role of data integrity in current good manufacturing practice (cGMP). The primary expectation is for data to be accurate and reliable. It does not establish legally enforceable responsibilities, but rather describes the FDA's current thinking. It is not a required document to adhere to, but it is advisable to be familiar with the text.

Key technical terms used in this document include:

- **Static record format**, where static indicates a fixed data document such as a paper record or electronic signature.
- **Dynamic record format**, which means a record that allows interaction between the user and record content, such as entering values manually in the system database.
- For a **computer or related system**, the "system" refers to the ANSI definition, which includes people, machines and methods organized to accomplish a set of specific functions. In addition, this system can include compute hardware, software, peripherals, networks, cloud infrastructure, operators and documents (manuals, SOPs, etc.)

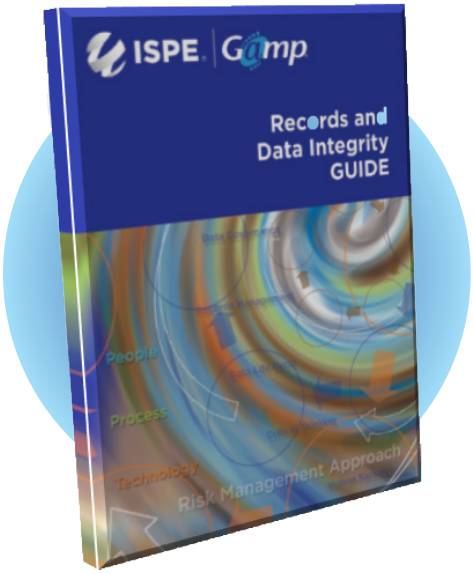
MHRA GxP Data Integrity Guidance

The guidance document produced by the United Kingdom emphasizes that data integrity is fundamental to ensuring that medicines are of the required quality in a pharmaceutical quality system. The result of effective, robust data governance is complete, consistent and accurate data used throughout the system.

The MHRA Inspectorate Blog[10] had this helpful quote:

> ***"A senior management resolution for the new financial year might be put to good use by reviewing the suitability of current performance metrics and engaging with front line staff in an attempt to understand the challenges of their day to day operations. By doing so, employees feel connected with management and feel that their voices, however inexperienced they may be, are heard and valued."***
>
> CHURCHWARD, MHRA INSPECTORATE

Recommended Reading



The ISPE Gamp Guide[11] addresses paper records, electronic records, and hybrid situations, while encouraging a move away from hybrid situations, wherever practical. The impact of record and data integrity issues can be significant on a regulated company, and can result in recalls of products, warning or untitled letters, import alerts, injunctions, seizures, Application Integrity Policy Invocations/ legal action, and ultimately the potential for patient harm. These regulatory actions can also have a significant financial impact.

The approach described in the guide is intended to encourage innovation and technological advances while avoiding unacceptable risk to product quality, patient safety, and public health.

Ethics

The importance of integrating ethics into the data integrity approach cannot be understated. From the PDA Journal[12]:

> ***"The prevention of data integrity breaches can be addressed with three primary elements: Personnel and Training, a Validation Program, and Security...***
>
> ***...Company standards of ethical conduct are defined to be followed, assuring that each employee acts with integrity in the execution of their work...***
>
> ***...Each employee is responsible for the validity and integrity of their data and documentation, whether it is a paper-based or electronic system."***
>
> PDA POINTS TO CONSIDER: FUNDAMENTAL CONCEPTS IN DATA INTEGRITY

To safeguard against unethical behavior, it is recommended that data manipulation not be allowed, that all records are created automatically (and not created after the fact from memory) and retain their unchanged time information, that all pertinent data is included (even if it is undesirable), that no passwords are shared between personnel, and that all original records are stored and kept safely on non-volatile media and never discarded or destroyed.

Conclusion

Everyone involved in the process, no matter their position, is responsible for upholding data integrity. Data Integrity is a significant component of the Quality Management System, and inspectors around the world have made it very clear that good intentions are no defense against compromised data.

The pharmaceutical industry must strongly consider any preventive or corrective action to improve product quality through an honest, ethical approach to data collection and retention.

References

1. FDA. (2006, June 30). The History of Drug Regulation in the United States. *Retrieved from https://www.fda.gov/downloads/AboutFDA/WhatWeDo/History/ProductRegulation/PromotingSafeandEffectiveDrugsfor100Years/UCM114468.pdf*
2. PharmaCompass. (2017, January 19). 2016 - A Year of Data Integrity Issues and Pharma Non-Compliances. *Retrieved from http://www.pharmacompass.com/radio-compass-blog/2016-a-year-of-data-integrity-issues-and-pharma-non-compliances*
3. 2016 Warning Letters. (2016). *Retrieved from https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2016/default.htm*
4. MHRA. (2016, April). MHRA GMP Inspection Deficiency Data Trend 2016. *Retrieved from https://mhrainspectorate.blog.gov.uk/2017/04/21/2016-gmp-inspection-deficiency-data-trend/*
5. FDA. (1997, March 20). Title 21 of the Code of Federal Regulations Part 11. *Retrieved from https://www.ecfr.gov/cgi-bin/text-idx?SID=86f097b6d76ecd7a285c372810e22a9f&mc=true&node=pt21.1.11&rgn=div5#se21.1.11_1300*
6. Committee on National Security Systems. (2010, April 26). National Information Assurance (IA) Glossary.
7. South, G. (2018, February 26). Ensuring data integrity through ALCOA. *Retrieved from https://www.pharmout.net/data-integrity-alcoa/#*
8. European Commission, EudraLex. (2011, January). Annex 11: Computerised Systems. *Retrieved from https://ec.europa.eu/health/documents/eudralex/vol-4_en*
9. FDA. (2016, April). Data Integrity and Compliance with cGMP Guidance for Industry (Draft Guidance). *Retrieved from https://www.fda.gov/downloads/drugs/guidances/ucm495891.pdf*
10. Churchward, D. (2017, March 30). Too much pressure: A behavioural approach to Data Integrity (Part 2). *Retrieved from https://mhrainspectorate.blog.gov.uk/2017/03/30/too-much-pressure-a-behavioural-approach-to-data-integrity-part-2/*
11. ISPE. Guidance Documents. *Retrieved from https://ispe.org/publications/guidance-documents*
12. Buhlmann, B., Dole, M., & Kaufmann, Z. (2016). PDA Points To Consider: Fundamental Concepts in Data Integrity. PDA Journal of Pharmaceutical Science and Technology, 70(5), 482-488. doi:10.5731/pdajpst.2016.007062.

Author

Daniele Pandolfi

Life Sciences, Aerosol Product Line Manager
Particle Measuring Systems

Daniele Pandolfi has had experience in particle counter instrumentation and cleanroom contamination control for over ten years. While building strong customer relationships, he has helped many people solve their cGMP issues. Outside of work, he is a semi-professional photographer, an enthusiast of electronics, a lover of new technology, and a keen traveler.

Edited by Briana Krueger, Technical Writer at Particle Measuring Systems