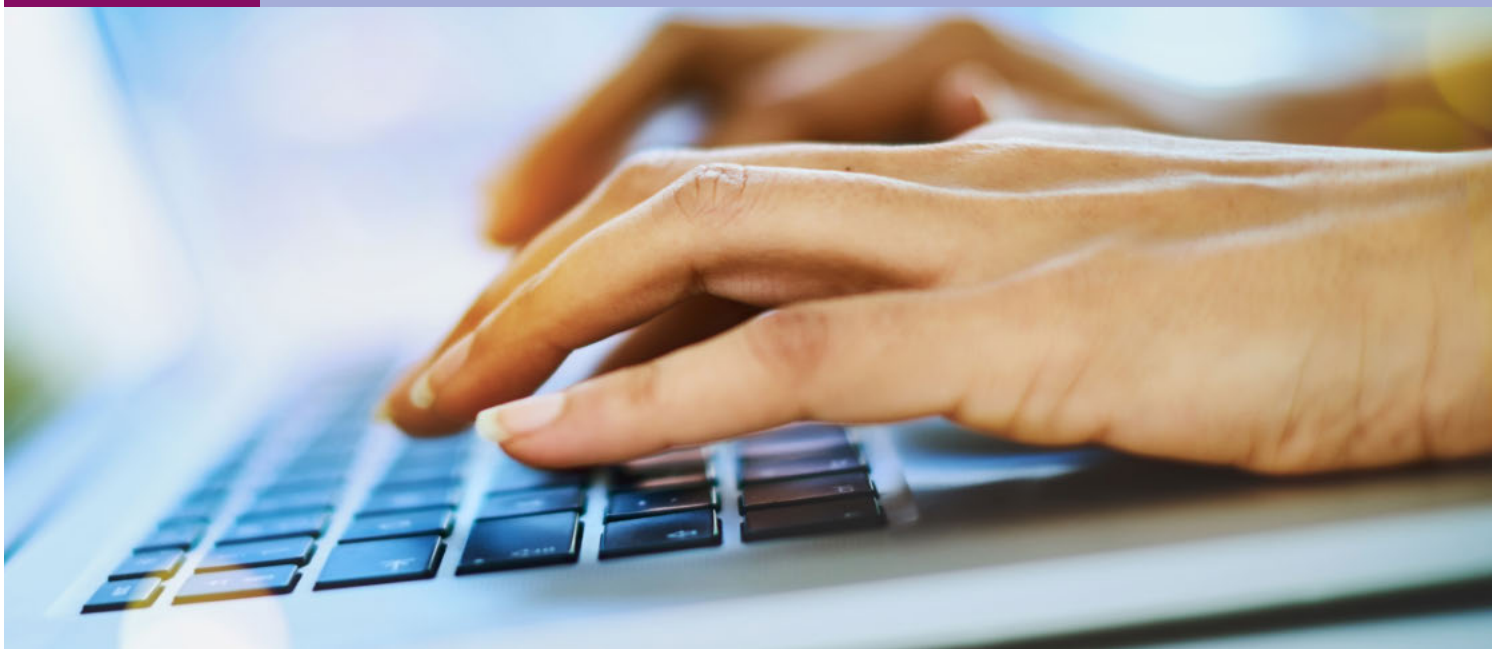
WHITE PAPER

Data Integrity: What is it and Why is it Important?



Introduction

After two and a half years of releasing a draft version, in December 2018, the U.S. Food and Drug Administration (FDA) published the finalized guidance document entitled "Data Integrity and Compliance with Drug CGMP". Through the response of the public's comments, the agency offered more details around their thinking of current best practices for the "design, operation and monitoring of systems to maintain data integrity.[1] The aim for this document was to give clarity of data integrity's role in Current Good Manufacturing Practice (CGMP), as required in 21 CFR parts 210, 211, and 212. The FDA has always maintained the goal of drug manufacturers ensuring data is complete, consistent, and accurate, and therefore trustworthy and reliable. The published guidance is intended to assist manufacturers in addressing prominent identified data integrity gaps. It points towards implementation of best practices, to address issues that can create risks to the reliability and the integrity of data produced.

It is important that there is an understanding of how data integrity is defined when considering establishment of a compliant working environment and process. The FDA defines data integrity as "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)".[2] ALCOA itself has evolved to ALCOA Plus, which incorporates two of the fundamental definition terms as stated by the FDA; complete, consistent, enduring and available.

FDA Warning Letters

The drug manufacturing environment has evolved, bringing new technologies and more computerized systems. However, this has brought more challenges to the agencies for oversight to these advanced opportunities. The guidance document was issued in reaction to 'increasingly observed CGMP violations involving data integrity during CGMP inspections", which consequently "led to numerous regulatory actions, including warning letters, import alerts and consent decrees". Data has been reported and collected for the last several years on the number of warning letters which have data integrity components to them. In the past six years, there has been a steady increase in the observance of these warning letters. Reviewing this data from 2013-2018 (10 warning letters in 2013 compared with 54 in 2018), a 540 % increase in warning letters issued with a data integrity component has been reported.[3] Inspectors continue to increase scrutiny of data trustworthiness as ensuring data integrity in CGMP environments is a crucial aspect of agency's responsibility to ensure the safety, efficacy, and quality of drugs, and to safeguard public health.

PerkinElmer®
For the Better

As recent as 2018, data integrity violations, which became a part of issued warning letters, covered 58 % (54) of the 95 total warning letters issued. Findings do not seem to rest in one geographical location. The FDA maintains a jurisdiction of safety and compliance for any company which produces and intends to import or sell a drug product into the US. Outside the US, 60 % (44/73) of warning letters issued in 2018 had a data integrity component, compared with 45 % (10/22) of warning letters in the US. Regions outside the US which have routinely topped the list of having the higher percentage of warning letters with data integrity components include China and India. The final guidance document provides a question and answer format with 18 questions and FDA suggested responses, including explanations of the main terminologies used during CGMP inspections. It reflects the FDA's current thinking on the creation and management of data in accordance with CGMP requirements.[2-4]

Why is Data Integrity Important?

Data integrity is crucial throughout the entire CGMP data life cycle to guarantee traceability, accuracy and reliability. This applies to the creation, modification, processing, reporting, archival, retrieval, transmission and disposition of data after the record's retention period ends (Figure 1). System design and controls should protect original data against accidental and intentional modifications, falsification, and loss or deletion, throughout its life cycle.[2]

Unprotected data can result in loss of data and business continuity, drug product quality and recall risk, potential adverse reactions in patients (resulting from inadequate product quality or safety), downtime of production lines, undermine assurance of pharmaceutical quality, and break down basic trust between regulators and the general public.

ALCOA is an acronym, frequently used by the FDA, relating to both paper and electronic records (Figure 2).[2] ALCOA has been expanded to ALCOA Plus to include the crucial terms complete, consistent, enduring, and available (Figure 3 and Table 1). The first two terms are the foundation to the general definition of data integrity. Enduring allows for the record to be kept over time in its original state and maintaining data availability is important not only during inspections but also for reworking steps in a process if required.[5]

Figure 1. Data life cycle.

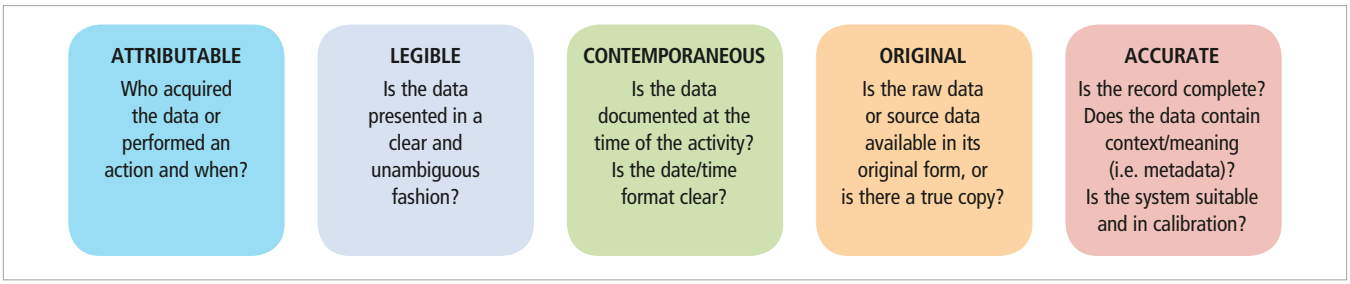


Figure 2. ALCOA data quality acronym.

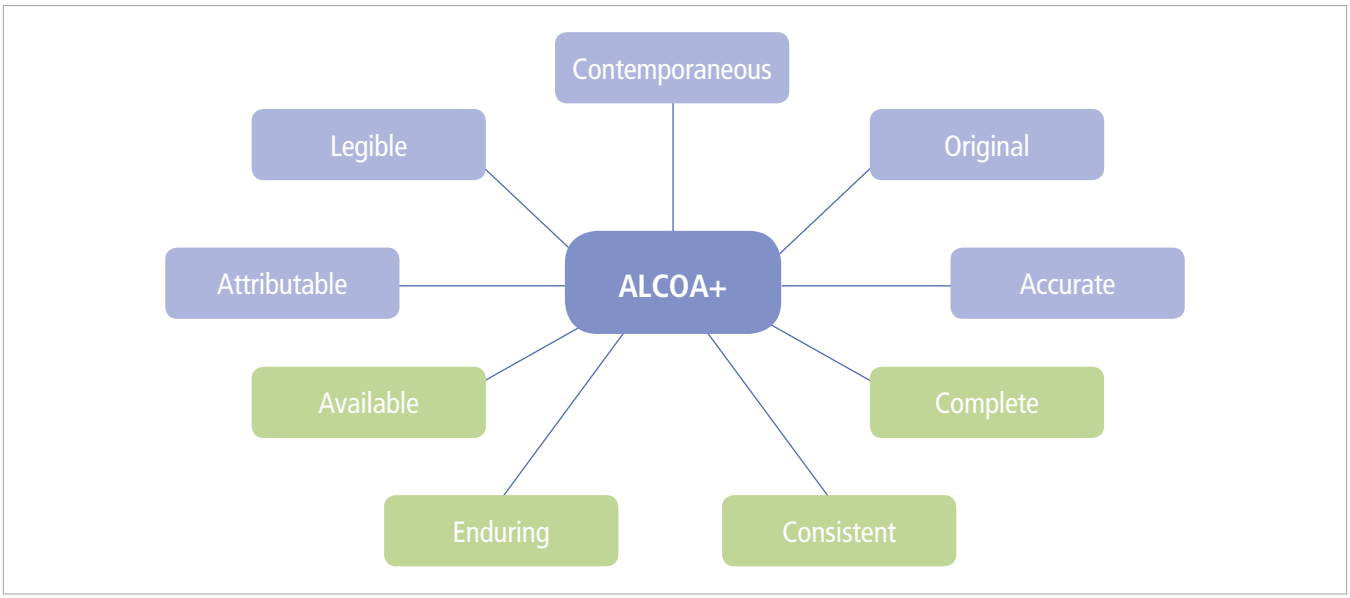


Figure 3. ALCOA Plus data quality acronym.

Table 1. Directive/SOP/work instructions for the respective ALCOA Plus dimensions of data integrity.[5]

Filter	Cost/Filter
Attributable	Access Control, Audit Trail Design, Date and Time, Electronic Signatures, GDP
Legible	Good Document Practices
Contemporaneous	Date and Time, Good Documentation Practices, Audit Trail
Original	Raw Data and Metadata retention, electronic lab notebook (if used), Document control (use of forms or notebooks should be controlled in a systematic manner to record original data)
Accurate	Calibration, Laboratory controls, Change Control, Deviation and Incident management, Validation, Out-of-Specification
Complete	Laboratory Controls, Good Documentation Practices, Manual data entry, Audit Trail Rules
Consistent	Validation, Audit Trail Review, system development life cycle (SDLC), GxP Records management, Manual Integration guidance, Out-of-Specification
Enduring	Data Backup and Recovery, Audit Trail Design, Building Monitoring System design, Data Migration and Archiving, Business Continuity
Available	Data Backup and Recovery, Data archiving, Building Monitoring System design

Key areas the FDA has routinely placed focus on include access controls, audit trails, and complete validations of systems. Reliability in the data created, reported, approved and used to release a product can be proved by providing evidence in the form of policies, procedures and controls, together with documented proof that each has been tested for its intended purpose (as written into the policy or procedure). This reliability establishes trust in the data's integrity throughout the data life cycle. Elimination or complete neglect to these items shows the agency a lack of commitment to the quality and integrity of the data produced.

When working with a computerized system, it is required to establish documented evidence which provides assurance that the System will consistently produce results which meet its predetermined requirements, specification and quality. Understanding how the instrument will be used, the risks associated with functions and what requires a validation is the responsibility of the end user prior to allowing that system to release data in a GMP environment. Key features as mentioned above, access control and audit trails must be understood and tested.

CGMP for Drugs

CGMP for drugs (21 CFR parts 210, 211, and 212) requires companies "to use technologies and systems that are up-to-date in order to comply with the regulations". FDA's authority for CGMP originates from section 501(a)(2)(B) of the Federal Food, Drug, and Cosmetic Act (FD&C Act).

In recent years, regulatory agencies have determined that electronic data is more secure and less likely to be manipulated when tracking the lifecycle of products and processes. Electronic data does, however, need to be compliant with Chapter 21 Code of Federal Regulations Part 11 and the European Union law EDQM Annex 11.

Some key requirements with respect to data integrity for CGMP include:

- Documentation at time of performance
- Data should be "stored to prevent deterioration or loss"
- Backup data needs to be exact, complete and secure from alteration, inadvertent erasures, or loss
- Records should be retained as "original records", "true copies" or other "accurate reproductions of the original records"
- Complete records of all data

CGMP-compliant record-keeping practices, such as audit trails, prevent data from being lost or obscured and ensure documentation at the time of performance.[3] This also demonstrates compliance to Data Integrity, as ALCOA states.

21 CFR Part 11 and EU GMP Annex 11

The FDA's regulation on Electronic Records and Signatures (21 CFR Part 11), and the European Medicine Agency's Guidelines to Good Manufacturing Practice – Annex 11: Computerized systems (EU GMP Annex 11) are two essential resources available to regulated life-science industries regarding correct data management. Each document has a strong focus on record accuracy, integrity, security and retrieval of data. However, they are not completely aligned.[6]

EU GMP Annex 11 provides guidance to the industry and defines the criteria for managing electronic records and signatures. 21 CFR Part 11, on the other hand, is a U.S. federal regulation which establishes fully enforceable requirements under federal law regarding integrity, reliability and consistency of electronic signatures and records.[6-9] The regulation comprises three subparts:

1) 'Subpart A – General Provisions' covers the scope, implementation, and definitions of the regulation.
2) 'Subpart B – Electronic Records' covers controls for open and closed systems, and electronic signature attributes.
3) 'Subpart C – Electronic Signatures' covers the requirements and controls governing signature usage.

Although the criteria for compliance with 21 CFR Part 11 is quite extensive, the main facets which must be adhered to include, but are not limited to:[8]

Logins

21 CFR Part 11.10 (d) highlights that compliant software systems must be 'limiting system access to authorized individuals'. This means a unique User Name and Secret Password is required for all authorized users.

Permissions

21 CFR Part 11.10 (g) emphasizes that the software must 'use authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.' This means there must be different groups with different accessibility levels. Examples may include System Admin, General User, Super User.

Electronic Signatures

21 CFR Part 11.100 (a) states that 'each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else'. An electronic signature, as defined by 21 CFR Part 11, means 'a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.' Electronic signatures are not compulsory under 21 CFR Part 11 but their use is strongly recommended. A user name, timestamp, and hierarchy of privileges should be included in the electronic signature.

Protection of Records

21 CFR Part 11.10 (c) indicates that the software must have 'Protection of records to enable their accurate and ready retrieval throughout the records retention period'. Essentially, all data collected and generated inside the software must be maintained securely, with adequate provision for ease of its retrieval.

Audit Trails

Audit trails are required for all systems which record GxP data to ensure traceability. 21 CFR Part 11.10 (e) maintains that the software must use 'secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying'.

References

1. Press Release Statement, Food and Drug Administration, Scott Gottlieb, M.D, December 2018. https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm628244.htm Date accessed: March 2019.
2. *Data Integrity and Compliance with Drug CGMP: Questions and Answers; Guidance for Industry,* Food and Drug Administration, 2018.
3. B. Unger, An Analysis of FDA FY2018 Drug GMP Warning Letters, Pharmaceutical Online, February 2019, https://www.pharmaceuticalonline.com/doc/an-analysis-of-fda-fy-drug-gmp-warning-letters-0003. Date accessed: March 2019.
4. https://www.manufacturingchemist.com/news/article_page/New_FDA_guidance_on_data_integrity_and_CGMP_compliance/121415. Date accessed: Feb 2019.
5. The 5P Model for Data Integrity, Institute of Validation Technology, 2018. Available from: http://www.ivtnetwork.com/article/5p-model-data-integrity.
6. D. Pandolfi, *Application Notes and Whitepapers Supplement 2018, European Pharmaceutical Review, 2018,* 23, 24-25.
7. *Comparison of 21 CFR Part 11 and Annex 11 of EU Guidelines to GMP,* UL PURE Learning, 2018. Available from: https://www.ulpurelearning.com/hubfs/GDPRzone/Annex11_Part11_WP_v8.pdf.
8. *Electronic Records; Electronic Signatures,* 21 C.F.R., § 11 (2019).
9. *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application,* Food and Drug Administration, 2003.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

PerkinElmer®

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs

014730_01 PKI