Data Integrity– a current „Hot Topic“ of the authorities

Requirements of 21 CFR Part 11, Annex 11 and other relevant guidelines

Content of the presentation

Approximately 35% of all Warning Letter in 2017 include observations regarding the integrity of data.

Paper based data are concerned as well as electronic data.

Therefore two major aspects will be discussed during this presentation:

- What is data integrity?
- What are the prerequisites to consider electronic equivalent to paper data?

In case paper based data are equal to electronic date, the requirement regarding data integrity are applicable to paper based data and electronic data.

Respective regulations

Document:	Content of the document
21 CFR Part 11 (1997)	Equivalence of paper based data and electronic data
Annex 11 of EU GMP regulations (2011)	Equivalence of paper based data and electronic data; CSV; Live Cycle Management of computerized systems
Data Integrity and Compliance with CGMP; FDA 2016 (Draft)	Explanations and description of various data integrity aspects and respective requirements
MHRA GxP Data Integrity Definitions and Guidance for Industry (03/2018) (Draft)	Explanations and description of various data integrity aspects and respective requirements
PIC(S: PI 041-1 (Draft 2) 10 August 2016	GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

Equivalence of paper based data and electronic data

Regarding the storage and archiving of electronic data you can distinguish between

Closed systems and

- The access to closed systems is allowed by the organization which is also responsible for the content of the system:
  - Intranet
  - Stand-alone PC

Open Systems

- The access to open systems is allowed by an organization which is not responsible for the content of the system:
  - Facebook
  - Internet

http://www.alegri.de/de/Sectors/Lists/WhitePapers/Alegri_Whitepaper_Cloud_Computing.pdf

Equivalence of paper based data and electronic data

Electronic Data:

- Validated system
- Correct and complete copies
- Protection against loss of data
- Permissions and Access Control
- Audit trail
- Workflow
- Use of tokens etc.
- System training
- Checks and controls about who is using the system

Paper-based Data:

- Validated processes
- Approved photo copy
- Archive
- Archive
- GMP compliant documentation
- Defined procedures
- 4-Eye principle
- Training
- Distribution lists

Equivalence of paper based data and electronic data / electronic signature

Electronic data:

- Control of system changes
- Electronic signature has to be undeletable associated with the data set
- Electronic signature has to identify the individual; signature needs two independent components. Signature has to stay unique

Paper-based data:

- Change Control
- Manual signature with permanent ink; GMP compliant documentation
- Manual signature; no printed signature; passport etc.

Conclusion: Electronic data and paper-based data can be looked at as equivalent to paper-based data and manual signature

Annex 11 requirements

Annex 11 is much more extensive than 21 CFR Part 11. Annex 11 considers for example GAMP 5. Annex 11 covers for example the following topics:

- Risk management
- Personal: Close cooperation between supplier of the system, QP, IT, system owner and any service provider
- QA Agreements between supplier / service provider and the respective company necessary
- If requested , the quality system of the supplier has to be shown during GMP inspections
- Complete list of computerized systems has to be available including the respective validation status
- Life Cycle Management
- Validation of the system including respective data migration
- Back-ups and restore of data

Data Integrity

What exactly is data integrity? Why is this a „hot topic“?

FDA has issued numerous 483s, regarding the observation, that

- Electronic data couldn‘t be reproduced correctly and completely
- Data got lost over time and haven‘t been readable anymore
- Haven‘t been captured in a timely manner
- Haven‘t been always complete
- Permissions for data processing haven‘t been defined adequately

Your firm does not exercise appropriate controls over computer related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel [21 C.F.R. 211.68(b)]. For example:

- Your “Processed By” dates and times listed on printed chromatograms do not always show the same “Processed By” dates and times listed on the system chromatograms.
- Your data in the audit trails does not always show the same data listed on your printed chromatograms.

Limiting access to or copying of records

Your firm limited access to or copying of records that our investigators were entitled to inspect. For example, our investigators requested records of your audit trail data from all chromatographic systems used to test drugs for the U.S. market at your facility. The files you ultimately provided (in the form of Excel spreadsheets rather than direct exports from your chromatographic software) were not the original records or true copies, and showed signs of manipulation. The records you did provide contained highlighting, used inconsistent date formats, and lacked timestamp data; these features are inconsistent with original data directly exported from chromatographic testing software.

Datenintegrität: Definition

Data Integrity: Explained in 180 seconds!!!

Data Integrity: Definition

So what is the definition of data integrity?

The extent to which all data are complete, consistent and accurate throughout the data lifecycle. (MHRA 2016)

Data integrity refers to the extend of the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be **a**ttributable, **l**egible, **c**ontemporaneously recorded, **o**riginal or a true copy, and **a**ccurate (**ALCOA**) (FDA 2016).

Data Integrity Requirements (MHRA 2016) - I

Die MHRA defines in the revised 2016 published draft the following requirements regarding:

- Data: Have to comply with the ALCOA principle
- Raw data must permit the full reconstruction of the activities resulting in the generation of the data.
- Metadata: Metadata is data that describe the attributes of other data, and provide context and meaning. Data without metadata are useless (compare result vs method) For example the bare information „NaCl“ on a sample label doesn‘t mean anything, if nothing is said about when the sample is taken by whom or from which lot and container.
- Data Governance: The sum total of arrangements to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle ; „Data Governance“ can looked at as the quality system to assure data integrity. Such a system has to available and described.

Data Integrity Requirements (MHRA 2016) - II

Die MHRA defines in the revised 2016 published draft the following requirements regarding:

- Data Lifecycle: All phases in the life of the data (including raw data) from initial generation and recording through processing (including analysis, transformation or migration), use, data retention, archive / retrieval and destruction. All those pahses have to be controlled based on written procedures (SOPs).
- Data migration: Data transfer/migration should be designed and validated to ensure that data integrity principles are maintained (not just the system itself)
- Data Processing: When used, data might be processed for various purposes. Data Processing has to be traceable throughout the life time of the data (audit trail). All processing activities have to be traceable from the data and the audit trail.

Data Integrity Requirements (MHRA 2016) - III

Die MHRA defines in the revised 2016 published draft the following requirements regarding:

- Data collection: Organizations should have an appropriate level of process understanding and technical knowledge of systems used for data collection and recording, including their capabilities, limitations and vulnerabilities
- Data Excluding: Data may only be excluded where it can be demonstrated through valid scientific justification that the data are not representative of the quantity measured, sampled or acquired.
- Original Record / True Copy: Data (specifically electronic data) should be available as original data as well as „True Copy“.
- Computer Transactions: When using electronic systems, data are not always immediately stored (cache). Critical data should be stored immediately during data collection whenever possible. (Paper: timely documentation).

Data Integrity Requirements (MHRA 2016) - IV

Die MHRA defines in the revised 2016 published draft the following requirements regarding:

- Audittrail: "*Audit trails are metadata that are a record of critical information (for example the change or deletion of relevant data) that permit the reconstruction of activities*." The audit trail has to show who did which activities when. It should not be able to shut down the audit trail. It has to be assured, that the audit trail can be reviewed. Audit trail review should be done on a lot by lot basis (is already required by the FDA) .
- Electronic Signature: 21 CFR Part 11 provides all relevant requirements
- Data Review: Data have to be reviewed for batch release based on the original data or a True Copy (what is a TrueCopy?).

Data Integrity Requirements (MHRA 2016) - V

Die MHRA defines in the revised 2016 published draft the following requirements regarding:

- Access and permissions: Requirements are described in detail in 21 CFR Part 11 and Annex 11.
- Data Retention: Data have to be archived in a safe and protected archive or as a secure back-up.
- Archiving of data: Archived data have to be able to reproduce any activities and results since the time those data have been developed.
- Back-up: Back-op and restore procedures have to be defined in an SOP and have to be validated on a routine schedule.
- Validation – for it‘s intended purpose: In contrast to other validation documents, it is not recommended to buy validation documents from the supplier of the software. What is the reason?

Data Integrity Requirements (MHRA 2016) - VI

Die MHRA defines in the revised 2016 published draft the following requirements regarding:

- Cloud applications (open systems; currently not frequently used by pharmaceutical companies but will be in the future). When cloud applications will be used, the following topics have to be considered:
  - Geographical position of the Cloud storage and respective lows applicable in this country
  - QAA between the company and the „cloud supplier“ covering all data integrity aspects
  - Access to data have to be assured at any time (inspections)
  - Back-up and Restore
  - Validation of the cloud solution
  - Business-Continuity agreements (validation!!!)

Data Integrity Requirements (MHRA 2016) - VII

What any company should be able to show:

- An overall SOP or policy describing the companies understanding regarding data integrity, which guidelines the company took into consideration for implementing data integrity measures and how the requirements described have been implemented for paper-based data and electronic data.
- References to more detailed SOPs

Any questions?
Thank you for your attention!