Regulatory Update – Data Integrity

Stefan Wurzer, Global Data Integrity Lead, Roche

Agenda and Learning Objectives

- **Overview about Data Integrity and Data Governance**
  - Understand what Data Integrity and Data Governance is about
- **Essential Requirements / Update Guidelines Changes**
  - Understanding essential Data Integrity requirements and guidelines
- **Inspection Findings / e.g. Warning Letters**
  - Identifying current focus areas related to Data Integrity by reviewing common inspection findings

Overview about Data Integrity and Data Governance
Definitions

"Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle." (WHO, 2016)

"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). (FDA, 2016)

"Data governance systems should be integral to the pharmaceutical quality system. It should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity, including control over intentional and unintentional changes to, and deletion of information." (PIC/S, 2016)

"The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate." (MHRA, 2018)

Essential Requirements / Update Guidelines Changes

Overview Key Guidances and Requirements

- **WHO:** DRAFT Guidance on Good Data and Record Management Practices (2016)
- **FDA:** DRAFT Data Integrity and Compliance with CGMP Guidance for Industry (2016)
- **European Medicines Agency:** Q&A Data Integrity (2016)
- **PIC/S:** DRAFT Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments (2016, **under revision**)
- **MHRA:** 'GXP' Data Integrity Guidance and Definitions (2018, **revised**)

Essential Requirements / Update Guidelines Changes

WHO DRAFT Guidance (2016) - Contents

- Quality risk management to ensure good data management
- Management governance and quality audits
- Contracted organizations, suppliers and service providers
- Training in good data and record management
- Good documentation practices
- Designing and validating systems to assure data quality and reliability
- Managing data and records throughout the data life cycle
- Addressing data reliability issues

Essential Requirements / Update Guidelines Changes

WHO DRAFT Guidance (2016) - Examples of Requirements

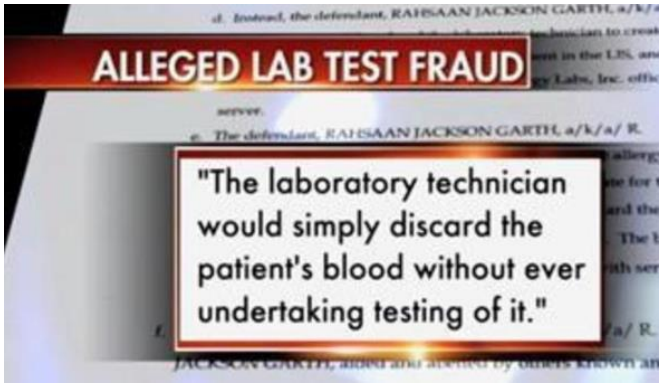
Related to Quality Culture:

- Management, with the support of the quality unit, should establish and maintain a working environment that minimizes the risk of non-compliant records and erroneous records and data
- An essential element of the quality culture is the transparent and open reporting of deviations, errors, omissions and aberrant results at all levels of the organization, irrespective of hierarchy
- Steps should be taken to prevent, and to detect and correct weaknesses in systems and procedures that may lead to data errors so as to continually improve the robustness of scientific decision-making within the organization

Essential Requirements / Update Guidelines Changes

FDA DRAFT Guidance (2016) - Contents

- Audit Trail Review
- “Static” vs. “Dynamic” Data
- Backup of systems
- Decision making CGMP data (exclusion criteria)
- Validation for its intended use
- User Access Controls (Individual log-ins, segregation of duties)
- Controls for blank forms
- True Copies
- Electronic Records
- Electronic Signatures
- Testing into Compliance



Clarifies the role of data integrity in current good manufacturing practice (CGMP) for drugs, as required in 21 CFR parts 210, 211, and 212.

Requirements with respect to data integrity in parts 211 and 212 include, among other things:

- § 211.68 (requiring that "backup data are exact and complete," and "secure from alteration, inadvertent erasures, or loss");
- § 212.110(b) (requiring that data be "stored to prevent deterioration or loss");
- §§ 211.100 and 211.160 (requiring that certain activities be "documented at the time of performance" and that laboratory controls be "scientifically sound");
- § 211.180 (requiring that records be retained as "original records," "true copies," or other "accurate reproductions of the original records"); and
- §§ 211.188, 211.194, and 212.60(g) (requiring "complete information," "complete data derived from all tests," "complete record of all data," and "complete records of all tests performed")

Essential Requirements / Update Guidelines Changes

FDA DRAFT Guidance (2016) - Examples of Requirements

Related to User Access Controls:

- Appropriate controls to assure that only authorized personnel make changes to computerized Master production & control records, or other records, or input laboratory data into computerized records
- FDA suggests that the system administrator role, including any rights to alter files and settings, be assigned to personnel independent from those responsible for the record content
- Implement documentation controls that ensure actions are attributable to a specific individual (see §§ 211.68(b), 211.188(b)(11), 203 211.194(a)(7) and (8), and 212.50(c)(10))
- When login credentials are shared, a unique individual cannot be identified through the login and the system would thus not conform to the CGMP requirements in parts 211 and 212

Essential Requirements / Update Guidelines Changes

FDA DRAFT Guidance (2016) - Examples of Requirements

Related to Blank Forms:

- FDA recommends that, if used, blank forms (including, but not limited to, worksheets, laboratory notebooks, and MPCRs) be controlled by the quality unit or by another document control method
- Incomplete or erroneous forms should be kept as part of the permanent record along with written justification for their replacement (for example, see §§ 211.192, 211.194, 212.50(a), and 212.70(f)(1)(vi))
- Similarly, bound paginated notebooks, stamped for official use by a document control group, allow detection of unofficial notebooks as well as of any gaps in notebook pages

Essential Requirements / Update Guidelines Changes

FDA DRAFT Guidance (2016) - Examples of Requirements

Related to Audit Trail Review:

- FDA recommends that audit trails that capture changes to critical data be reviewed with each record and before final approval of the record
- Audit trails subject to regular review should include, but are not limited to, the following: the change history of finished product test results, changes to sample run sequences, changes to sample identification, and changes to critical process parameters
- Personnel responsible for record review under CGMP should review the audit trails that capture changes to critical data associated with the record as they review the rest of the record (for example, §§ 241 211.22(a), 211.101(c), 211.194(a)(8), and 212.20(d))

Essential Requirements / Update Guidelines Changes

EMA Guidance (2016) - Contents

- Data Risk and Data Criticality Assessments
- Data Life cycle management
- Controls for blank forms
- Designing and validating systems to assure data integrity
- Review of Electronic Data
- Self-Inspection Programs related to Data Integrity
- Contractor/vendor qualification/assurance program

Essential Requirements / Update Guidelines Changes

EMA Guidance (2016) - Contents

	Basic Requirements for Medicinal Products (Part I): Chapter 4[1] / Chapter 6[2]	Basic Requirements for Active Substances used as Starting Materials (Part II) : Chapter 5[3] / Chapter 6[4]	Annex 11 (Computerised System)
Attributable (data can be assigned to the individual performing the task)	[4.20, c & f], [4.21, c & i], [4.29, e]	[6.14], [6.18], [6.52]	[2], [12.4], [15]
Legible (data can be read by eye or electronically and retained in a permanent format)	[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]	[5.43] [6.11], [6.14], [6.15], [6.50]	[7.1], [9], [10], [17]
Contemporaneous (data is created at the time the activity is performed)	[4.8]	[6.14]	[12.4], [14]
Original (data is in the same format as it was initially generated, or as a 'verified copy', which retains content and meaning)	[4.9], [4.27], [Paragraph "Record"]	[6.14], [6.15], [6.16]	[8.2], [9]
Accurate (data is true / reflective of the activity or measurement performed)	[4.1], [6.17]	[5.40], [5.45], [6.6]	[Paragraph "Principles"],[5], [6], [10], [11]

[1]Chapter 4 (Part I): Documentation

[2]Chapter 6 (Part I): Quality control

[3]Chapter 5 (Part II): Process equipment (computerized system)

[4]Chapter 6 (Part II): Documentation and records

Essential Requirements / Update Guidelines Changes

EMA Guidance (2016) - Examples of Requirements

Related to Review of Electronic Data:

- Electronic data is the original record which must be reviewed and evaluated prior to making batch release decisions and other decisions relating to GMP related activities (e.g. approval of stability results, analytical method validation etc.)
- In the event that the review is based solely on printouts there is potential for records to be excluded from the review process which may contain un-investigated out of specification data or other data anomalies
- The review of the raw electronic data should mitigate risk and enable detection of data deletion, amendment, duplication, reusing and fabrication which are common data integrity failures
- Exception Reporting is used commonly as a tool to focus the review of electronic data such as (but not limited to) electronic batch records

Essential Requirements / Update Guidelines Changes

EMA Guidance (2016) - Examples of Requirements

Related to Self-Inspection Programs:

- Ongoing compliance with the company's data governance policy/procedures should be reviewed during self-inspection, to ensure that they remain effective

Essential Requirements / Update Guidelines Changes

PIC/S DRAFT Guidance (2016) - Contents

- Data Governance Systems
- Code of Ethics and policies
- Quality Culture
- Review of Quality Metrics
- Dealing with Data Integrity Issues
- General Data Integrity Principles and enablers
- Specific Data Integrity Considerations (paper based and computerized systems)
- Data integrity considerations for outsourced activities
- Regulatory actions in response to data integrity findings
- Remediation of data integrity failures

Essential Requirements / Update Guidelines Changes

PIC/S DRAFT Guidance (2016) - Examples of Requirements

Related to Data Governance:

- Data governance systems should be integral to the pharmaceutical quality system
- It should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity, including control over intentional and unintentional changes to, and deletion of information

  These controls may be:

  - Organisational (e.g. data governance system design, considering how data is generated, recorded, processed, retained and used, and risks or vulnerabilities are controlled effectively)
  - Technical (e.g. computerised system control)

Essential Requirements / Update Guidelines Changes

PIC/S DRAFT Guidance (2016) - Examples of Requirements

Related to Direct print-outs from electronic systems:

- Paper records generated by very simple electronic systems, e.g. balances, pH meters or simple processing equipment which do not store data provide limited opportunity to influence the presentation of data by (re-)processing, changing of electronic date/time stamps
- In these circumstances, the original record should be signed and dated by the person generating the record and the original should be attached to batch processing records

Essential Requirements / Update Guidelines Changes

PIC/S DRAFT Guidance (2016) - Examples of Requirements

Related to Remediation of Data Integrity Failures:

- Consideration should be primarily given to resolving the immediate issues identified and assessing the risks associated with the data integrity issues
- The response by the company in question should outline the actions taken. Responses should include:
  - A comprehensive investigation into the extent of the inaccuracies in data records and reporting
  - Corrective and preventative actions taken to address the data integrity vulnerabilities and timeframe for implementation
- A management strategy should be submitted to the regulatory authority that includes the details of the global corrective action and preventive action plan

Essential Requirements / Update Guidelines Changes

MHRA Guidance (2018) - Contents

- Principles of Data Integrity
- Establishing data criticality and inherent integrity risk
- Designing systems and processes to assure data integrity; creating the ‘right environment’.
- Data Governance
- Data Lifecycle
- Original record and true copy
- Audit Trail
- Electronic Signatures
- Computerised system user access/system administrator roles
- IT Suppliers and Service Providers

Essential Requirements / Update Guidelines Changes

MHRA Guidance (2018) - Examples of Requirements

Related to System Design:

- Systems and processes should be designed in a way that facilitates compliance with the principles of data integrity (i.e.:)
  - At the point of use, having access to appropriately controlled/synchronised clocks for recording timed events to ensure reconstruction and traceability, knowing and specifying the time zone where this data is used across multiple sites
  - Accessibility of records at locations where activities take place so that informal data recording and later transcription to official records does not occur
  - User access rights that prevent (or audit trail, if prevention is not possible) unauthorised data amendments

Essential Requirements / Update Guidelines Changes

MHRA Guidance (2018) - Examples of Requirements

Related to Audit Trail Review:

- It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.)
- Routine data review should include a documented audit trail review where this is determined by a risk assessment
- Audit trails may be reviewed as a list of relevant data, or by an ‘exception reporting' process
- An exception report is a validated search tool that identifies and documents predetermined ‘abnormal’ data or actions, that require further attention or investigation by the data reviewer
- Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata

Inspection Findings / e.g. Warning Letters

Analysis of 2017 FDA Warning Letters on Data Integrity

21 CFR Reference	Number of Times Cited	Title of CFR Section
211.188	9	Batch Production and Control Records
211.194	9	Laboratory Records, Review of All Data
211.22	8	Responsibitities of the Quality Control Unit
211.192	5	Production Record Review, Deviations, and Investigations
211.68	3	Automatic, Mechnical, and Electronic Equipment

FDA issued **82** warning letters in 2017. **56** included a Data Integrity component.

Source: Pharmaceutical Online, 18 May 2018, Barbara Unger

Data Integrity Remediation

Your quality system does not adequately ensure the accuracy and integrity of data to support the safety, effectiveness, and quality of the drugs you manufacture. We strongly recommend that you retain a qualified consultant to assist in your remediation. In response to this letter, provide the following.

A. **A comprehensive investigation into the extent of the inaccuracies in data records and reporting.** Your investigation should include:

A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, and systems to be covered by the assessment; and a justification for any part of your operation that you propose to exclude.

Interviews of current and former employees to identify the nature, scope, and root cause of data inaccuracies. We recommend that these interviews be conducted by a qualified third party.

An assessment of the extent of data integrity deficiencies at your facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies. Describe all parts of your facility's operations in which you discovered data integrity lapses.

A comprehensive retrospective evaluation of the nature of the testing data integrity deficiencies. We recommend that a qualified third party with specific expertise in the area where potential breaches were identified should evaluate all data integrity lapses.

Inspection Findings / e.g. Warning Letters

Examples of Recent FDA Warning Letters on Data Integrity

B. **A current risk assessment of the potential effects of the observed failures on the quality of your drugs.** Your assessment should include analyses of the risks to patients caused by the release of drugs affected by a lapse of data integrity, and risks posed by ongoing operations.

C. **A management strategy for your firm that includes the details of your global corrective action and preventive action plan.**

Your strategy should include:

A detailed corrective action plan that describes how you intend to ensure the reliability and completeness of all of the data you generate, including analytical data, manufacturing records, and all data submitted to FDA.

A comprehensive description of the root causes of your data integrity lapses, including evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. Indicate whether individuals responsible for data integrity lapses remain able to influence CGMP-related or drug application data at your firm.

Interim measures describing the actions you have taken or will take to protect patients and to ensure the quality of your drugs, such as notifying your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, drug application actions, and enhanced complaint monitoring.

Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of your company's data. A status report for any of the above activities already underway or completed.

Inspection Findings / e.g. Warning Letters

Examples of Recent FDA Warning Letters on Data Integrity

Your firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 211.194(a)).

When reviewing audit trails, our investigator observed unreported data from in-process tablet weight checks. You programmed your in-process weight checker not to report values that varied more than **(b)(4)**% from the tablet target weight.

In your response, you committed to suspend this procedure, investigate any such values, and perform a retrospective assessment of tablet weight checker data. However, your retrospective tablet weight assessment was limited to all rejected measurements from February 1 to March 15, 2017, and about 8,000 rejected measurements representing an unspecified percentage of the total number of rejected measurements from August 1, 2016, to February 1, 2017. There was no commitment to revisit equipment qualification(s) and process validation(s) to ensure they included complete data.

In response to this letter, as part of your retrospective tablet weight assessment, explain whether your findings impact data supporting tablet manufacturing equipment qualification and manufacturing process validation studies. Provide a summary listing of equipment qualification and process validation documents that you reviewed.

Inspection Findings / e.g. Warning Letters

Examples of Recent FDA Warning Letters on Data Integrity

Your firm failed to establish an adequate quality control unit with the responsibility and authority to approve or reject all components, drug product containers, closures, in-process materials, packaging materials, labeling, and drug products, and the authority to review production records to assure that no errors have occurred, or if errors have occurred, that they have been fully investigated. (21 CFR 211.22(a)).

Your quality unit failed to review high performance liquid chromatography (HPLC) assay data for release and stability of your **(b)(4)** product.

During review of your HPLC's electronic data, we discovered at least 100 "test" injections. Your analytical procedures and methods do not discuss "test" injections. Your laboratory supervisors did not review these injections prior to submitting the data packages for approval. You informed our investigator that, per procedure, your laboratory supervisors and quality unit only review the chromatograms printed and submitted to them by the analysts. Because your analysts did not print the chromatographic results of "test" injections, neither laboratory supervisors nor your quality unit reviewed these injections. Your procedure did not require review of the underlying electronic records or data by either laboratory supervisors or the quality unit to ensure their accuracy or completeness. Accordingly, your quality unit relied on incomplete data for batch disposition decisions. Your quality unit failed to ensure the adequacy of procedures for assessing the quality of your drug products.

We observed other examples of your quality unit's failure provide adequate data management and review procedures, including the following:

Your analysts performed manual integration of chromatograms without instructions that describe when manual integration is permitted and how it is to be done.

You did not have procedures for reviewing audit trails or electronic data for the Fourier-transform infrared spectroscopy or ultraviolet systems.

Inspection Findings / e.g. Warning Letters

Examples of Recent FDA Warning Letters on Data Integrity

Failure to exercise sufficient controls over computerized systems to prevent unauthorized access or changes to data, and failure to have adequate controls to prevent omission of data.

Our investigator observed that the audit trail feature was disabled on instruments you use for quality control testing of your API, including your high performance liquid chromatography system. Your analytical systems also lacked controls to prevent users from deleting or altering electronic data. For example, your quality assurance executive, who also performed your analytical tests, had administrator access to each system.

In your response, you committed to validating all computerized systems with incorporation of audit trails, restrictions on data, and user-access controls by March 31, 2018.

Your response is insufficient because it does not include interim control measures and procedural changes for the control and review of analytical data. You also do not specify who will have administrator privileges on your analytical instrument systems used for CGMP quality control testing.

In response to this letter:

provide a summary of your interim controls to prevent deletion and modification of data;

define the roles and responsibilities of personnel who have access to analytical instruments and data;

provide a standard operating procedure (SOP) that ensures that all quality control tests are performed by an analyst and receive second-tier review (e.g., by a manager) from a separate individual;

detail the associated user privileges for each analytical system;

provide a detailed summary of your procedural updates and associated training for user role assignment and controls; and provide detailed procedures for your review of audit trail data.

Inspection Findings / e.g. Warning Letters

Other Inspection Findings related Data Integrity

- Laboratory analysts are authorized to write and edit test methods and laboratory personnel have administrator access to electronic records, which cast doubt on the reliability of the company's recordkeeping. A lack of audit trail reviews intensified the agency's concerns regarding the integrity of the company's data
- Users with administrator level privileges which are configured with the ability to purge audit trails and delete data
- Paper printouts were considered to be the raw data
- Not implemented second person verification as interim control for systems under data integrity remediation
- Failure to prevent unauthorized access by allowing shared user accounts and passwords and lack of role-based security
- Results recorded on unofficial documents

Acknowledgements

Joseph C. Famulare, Genentech/Roche
Vice President, Global Quality Compliance and External Relations
(Review of presentation)