Data Integrity
Background, Regulatory Requirements and Inspection Overview

Hugh McMahon
Quality Operations Manager
Genzyme Waterford
Introduction

• Data integrity is mandatory for the regulated healthcare industry, as processing and disposition decisions regarding product quality, safety, efficacy, purity, and compliance with the applicable regulatory requirements are made based on data that is recorded and reported.

• Data Integrity has always been a requirement but has recently become a major concern for global regulatory authorities, resulting in a significant increase in regulatory observations in this area.

• FDA have issued 14 Warning Letters to Indian API manufacturers in the last 2 years and multiple other Warning Letters to China and Europe for issues regarding data integrity.

• 12 out of 13 FDA Warning Letters issued between November 2013 to July 2014 (to non US sites) had Data integrity issues as against 8 out of 26 in the previous year
What is Data Integrity?

• The accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. Data integrity is imposed within a system at its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines.

• Refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

• It is a critical aspect to the design, implementation and usage of any system which stores, processes or retrieves data.

• Data is recorded exactly as intended, and upon later retrieval, the data is the same as it was when it was originally recorded and data is complete, consistent and accurate.
Falsification and Fraud

• Appropriate systems may be in place to ensure data integrity, however if there are issues with individual or company integrity this can give rise to falsification of records and fraudulent data.

• **Falsification** - creating, altering, recording, or omitting data in such a way that the data do not represent what actually occurred.

• **Fraud** - Wrongful or criminal deception intended to result in financial or personal gain.

• Falsification of data is a major concern for regulators and a significant driver for the enhanced level of concern and scrutiny from regulators in the area of data integrity.
Applicable Regulations

- **Electronic Systems – Data Integrity Annex 11- EU GMP Guide.** Data storage integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. This data should be checked for accessibility, readability and integrity.

- **Part I Chapter 4 and Annex 11 and Part II** - Data integrity requirements applicable to: – API and FP manufacturers, including contract manufacturing – Testing units, including contract laboratories – outsourced GMP activities such as equipment qualification and calibration

- **Electronic Systems – Data Integrity Annex 11- EU GMP Guide.** Risk Management- Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, **data integrity** and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

- **21 CFR, Part 210 and Part 211**
Requirements to Ensure Data Integrity

All data should follow ‘ALCOA’ requirements:

- **Attributable** - Who performed an action and when? If a record is changed, who did it and why? Link to the source data.

- **Legible** - Data must be recorded permanently in a durable medium and be readable.

- **Contemporaneous** - The data should be recorded at the time the work is performed and date / time stamps should follow in order.

- **Original** - Is the information the original record or a certified true copy? Is all data present and available.

- **Accurate** - No errors in data or editing performed without documented amendments.
Consequences of Data Integrity Issues

- Patient death, chronic illness or disability.
- EU statements of non-compliance
- Consent Decrees, FDA Warning Letters
- Importation Ban(s)
- Loss of consumer and regulator trust/confidence, very difficult to recover
- Product applications review suspended
- Market and share price reduction
Examples of Data Integrity Breaches

• Recent New England Compounding Pharmacy incident in the United States, 64 patients died and over 750 were sickened from fungal meningitis as a result of sterility negligence and data integrity issues. Records showed compounding rooms as being properly cleaned when they had not been.

• FDA investigators found unofficial batch records for approximately 75 batches of injectable finished drug products torn in half in a waste area. Data indicated that some batches failed to meet the in-process visual inspection specifications of not more than 4% defects, while the official batch records for these batches stated that these batches had met the specifications. Uncontrolled documents indicated that up to 14% of vials had defects.

• Documenting microbial results on a Certificate of Analysis when there was no objective evidence to support that any testing was actually performed.
Other Breaches Noted by Agencies

• **Non contemporaneous recording**: Failure to record activities at the time when activity was performed. There is evidence that the records were signed by company personnel when the person was actually absent on that day.

• **Document back-dating**: Backdating stability test results to meet the required commitments.

• **Copy of existing data as new information**: Test results from previous batches were used to substitute testing for another batch or acceptable test results were created without performing the test.

• **Re-running samples to obtain better results**: Multiple analyses of assay were done with the same sample without adequate justification and in some cases samples were tested unofficially or as a trial analysis until desired test results were obtained.

• **Data fabrication and data discarding**: Original raw data and records were altered for e.g., by using correction fluid or manipulation of a poorly defined analytical procedure and associated data analysis in order to obtain passing results.
Inspection Focus Areas

**General**
- Company understanding of computerised system capabilities and transfer of data between systems
- Up to date listing of all relevant systems and GMP functionality
- Control of networked and standalone instruments
- Policies and procedures detailing processing and control of data

**Qualification**
- User Requirement Specification - should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact.
- Evidence of appropriate test methods and test scenarios for parameter limits, data limits and error handling
- Justification on the extent of validation and data integrity controls documented through risk assessment of the computerised system.
Inspection Focus Areas

*Configuration of systems – GxP functions*
- Security of the system and user access levels – appropriate segregation of duties
- Electronic signatures – use of individual and generic passwords

*Data*
- Data processing and review, accuracy checks
- Potential for data manipulation and deletion
- Repeat testing / replicate data
- Date / time stamp manipulation
- Criteria used to invalidate data
- Data transfer to systems - Checks that data are not altered in value and/or meaning
- Level of checking should be statistically sound
Inspection Focus Areas

Storage of data

• **Regular back-ups** of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

• **Archived data** should be checked for accessibility, readability and integrity. If changes are to be made to the system, then the ability to retrieve the data should be ensured and tested.

• **Audit trails** - Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions.

• **Vendors** - Assessment of competency of contractor to deliver expectations.

• **Change management** - Changes to a part of the system may pose a risk due to interdependencies.
  - Is Data Integrity included in risk assessments?
  - Is Data Integrity included in training programme?
  - Is Data Integrity included in self inspection programme? – need to justify frequency of periodic evaluation based on system criticality and complexity.
Inspection Observations - QC labs

- **Audit Trails** – For electronic data acquisition systems, audit trails are not available or are not enabled; therefore, there is no record of data modifications or deletions.

- **Unique User Logins** – Each user should have a unique username and password for both the analytical software and the operating system. This is essential for tracing work performed to a unique individual.

- **Date/time stamp**. There was no date/time stamp of printing on analytical reports from ‘system’ (chromatograms, methods and sample set data) to facilitate traceability and ensure integrity of the data.

- **User Privilege Levels** – Each data acquisition system should have defined user levels based on the role the user will have in the system. Examples of common user levels include analyst, supervisor, manager and administrator. Privileges assigned to each level should be clearly defined and commensurate with the requirements for each user type.
• **Control Over Electronic Systems** – Failure to establish adequate controls over computer systems to prevent unauthorized access or changes to electronic data. This can include failure to have mechanisms to prevent unauthorized user access to the system, and ability to rename, move, delete or not save file results.

• **Control Over Processing Methods** – Use of HPLC processing methods (including integration parameters) that are not defined or controlled. This includes the practice of manual integrations without justification or approval, and processing injections in the same sequence with different processing methods and integration parameters.

• **Unofficial “Test” Injections** – Some firms have been cited for injecting samples prior to beginning an official sequence. This practice results in essentially generating data for products, but not reporting the data.

• **Test Non Compliant** - Reporting on a CoA that batches meet test specification without actually performing the testing, or having any supporting data.
Inspection Observations - QC labs

- **Inappropriate data management** - Raw data for HPLC/GC runs which had been invalidated due to failed system suitability criteria were stored separately to the QC raw data packages and were not included in the review process. The ‘log for record of invalidated runs’ was not incorporated under the quality management system and invalidated runs were not always evaluated and documented.

- **Suspect data entry** - Entries made in training records, production logbooks and QC records were made by staff that the company biometric logging in record showed were not on site at the time that the entry was purported to have been made.

- **Deleted data** - Evidence of deleted data files were noted. A duplicate analysis file for the same samples on the same day was found within the file structure. There was no reference to the second file or any file deletion either in the test records or the system logbook.
Inspection Observations - Stability

• **Modification of data** - Initial records of secondary spots for TLC related substance tests were later re-annotated to indicate that no secondary spot had been identified.

• **Missing raw data** - Summary reports were presented to the inspector for which the supporting raw data could not be provided. Missing raw data and incorrect entries that were reviewed and authorised as correct.

• **Inappropriate Sample ID** - A number of sample sets and their associated injections in the stability laboratory were not all appropriately identified and carried non descriptive titles, such as “trial”
Inspection Observations - Production

• Operations personnel performing manufacturing steps without a batch record or a manufacturing form to document the results contemporaneously.

• Manufacturing batch records IPC checks ‘completed’ in advance of a testing interval

• Manufacturing personnel back dating official documents and signing on behalf of each other.

• Company maintaining duplicate versions of cGMP raw data records. Undesirable data was found to be changed in the official versions in order to meet specifications

• Using post-it notes to capture information and then transferring that to worksheets or formal documentation.

• The User Requirement Specification did not specifically state all the requirements for the machine and was not linked to any critical process parameters / variables
Ensuring Data Integrity and Successful Regulatory Inspections

• Understand regulatory requirements and concerns and inspectional approach

• Create overview document that outlines company understanding and approach to Data Quality Management

• Perform Gap Assessment against applicable requirements and implement remediation plan via QMS

• Apply Risk management throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality

• Create awareness of data integrity among all personnel so they can assist company with meeting and report concerns before they become fully fledged issues
Ensuring Data Integrity and Successful Regulatory Inspections

• Embed data integrity verification activities into internal audit processes and train your internal auditors to understand what to look for in order to detect data integrity deficiencies

• Implement appropriate Data Integrity governance program

• Seek external support to assure completely unbiased, third-party investigations and/or to enhance your internal investigation program

• Share knowledge and experience with other companies
Summary

• Data integrity is critical to ensure product quality, safety, efficacy, purity, and compliance with the applicable regulatory requirements.

• Significantly increased regulatory inspectional focus in this area.

• By understanding regulatory expectations and inspectional approach it is possible to implement effective systems to ensure data integrity and successful regulatory inspections.
Acknowledgements


- Data Integrity: A Regulator’s Perspective. Ciara Turley, HPRA, PDA Irish Chapter, Data Integrity Seminar, May 2015.

Questions?