Risk-Based Approach for the Assessment and Remediation of Data Integrity

Jim Gunning-Johnson and Johnson
Vidya Sagar-Deloitte & Touche LLP
IVT CSV Conference - April 2017
Agenda

- Interactive Discussion on Data Integrity Regulatory Requirements
  - What is data integrity?
  - Health Authority Expectations for Data Integrity
  - Why Data Integrity is important
  - Review of Data Integrity issues and FDA Warning Letters
  - Comparison of Data Integrity Guidance Documents

- Case Study (EU Annex11 & MHRA-Data Integrity)
  - Development of an Assessment Strategy
  - Risk-based GAP remediation strategy
What is Data Integrity?

- The extent to which all data are:
  - Complete
  - Consistent
  - Accurate

  Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)

- Throughout the Data lifecycle
  - Initial generation
  - Recording and processing
  - Use
  - Retention
  - Archiving
  - Retrieval
  - Destruction
Data integrity refers to the completeness, consistency, and accuracy of data.

Think “ALCOA”
- **Attributable**: Who & When
- **Legible**: Clearly understood, traceable and permanent
- **Contemporaneous**: Recorded as occurs
- **Original**: Documentation of executed work at the time it is executed
- **Accurate**: Factual or Truthful

ALCOA has been around since the 1990’s, is used by regulated industries as a framework for ensuring data integrity.
Ensuring data integrity through “ALCOA”

- **Attributable (Person)-** All Data generated must be attributable to person and this can be achieved by maintaining paper log (Conventional) and audit trails in (electronic system). Any changes to data set must be logged with person name and date and time along with old and new value.

For example:

- Changing configuration parameter on software should be made by an authorised user and the details of the change logged in an audit trail with person name/user ID.

- During a formal testing exercise, test results should be initiated and dated by the person executing/approving the test.
Ensuring data integrity through “ALCOA” (Cont..)

- **Legible (Old/New Value)**- Data recorded must be readable (legible) and permanent. Ensuring records are human readable and permanent throughout the data lifecycle.

For example:

- In conventional process GDP will always promote the use of indelible ink when documenting batch manufacturing records/test protocols, if we make corrections ensure a single line is used to strike old record before we update new record with initials.

- In electronic system old value and new value must reflect in audit trails throughout the data lifecycle.
Ensuring data integrity through “ALCOA” (Cont..)

- **Contemporaneous (Time Stamp)**-
  Data must be generated at real time and data should never be back dated, date and time stamps should stream in order of execution for the data.

For example:

- If executing a test protocol, tests should be performed and their results recorded in real time with date and time stamp for manual or automated testing.
Ensuring data integrity through “ALCOA” (Cont..)

- **Original (Native version)** original/primary data recorded for the first time. This could be an approved document. If we make any changes to original data always we need to work on source/original data by capturing version history.

For example:

- Always work on native version (primary data) to maintain source of truth

- If your native data is in hard copy and needs to be stored electronically, ensure a “original copy” is generated, the copy is verified for completeness and then migrated into the electronic system
Ensuring data integrity through “ALCOA” (Cont..)

- **Accurate (Error Free)** Data should be error free and complete, editing should not be performed without documenting and annotating the amendments.

For example:

- Master data or transaction data entered should be accurate without any error.

- Build accuracy checks into the design of the electronic system with allowed +/- limits.
The underlying premise in 210.1 and 212.2 is that CGMP sets forth minimum requirements to assure that drugs meet the standards of the Federal Food, Drug, and Cosmetic Act (FD&C Act) regarding safety, identity, strength, quality, and purity. 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”)
- 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”).
Why Data Integrity is important?

- Lack of data integrity can undermine the confidence in a product’s safety, efficacy and quality

- Data integrity issues can erode trust
  - Trustworthiness and reliability

- Data integrity issues can impact business
  - Product holds
  - Recalls
  - Non-approvals
  - Regulatory challenges – Warning Letters, Consent Decrees etc.

- FDA has issued numerous Warning Letters for Data Integrity over the past 4 years
Some Data Integrity Issues

FDA Warning Letters

In recent years, FDA has increasingly observed CGMP violations involving data integrity during CGMP inspections. These data integrity-related CGMP violations have led to numerous regulatory actions, including warning letters, import alerts, and consent decrees.

- Issues cited in Warning Letters
  - Data Manipulation
  - Backdating
  - Falsifying data
  - Lack of controls in computerized systems to prevent manipulation and deletion of data
  - Destroying original batch records
  - Not completing batch production and control records immediately after activities were performed
  - All employees had admin privileges and shared one user name
  - Failure to adequately investigate OOS results
  - No Audit trails or gaps in audit trails
  - No Periodic audit trails review
Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records (21 CFR 211.68(b)). Computer in your quality unit area did not have controls to restrict access and prevent unauthorized changes to data files and folders. All employees had access to your Annual Product Review (APR) spreadsheet. The desktop computer containing the APR was not locked. In your response, you committed to “reassessing the GMP” requirements for computer-based systems; you stated the systems would be “evaluated, checked and validated.” You did not include a timeline or specify a plan to review released batches and determine the impact of the deficiency.

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 acknowledge that you are using a consultant to audit your operation and assist in meeting FDA requirements. In response to this letter, provide the following.

- A comprehensive investigation into the extent of the inaccuracies in data records and reporting.

- 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.

- A management strategy for your firm that includes the details of your global corrective action and preventive action plan.
Failure to prevent unauthorized access or changes to data, and to provide adequate controls to prevent manipulation and omission of data. During the inspection, we observed that your laboratory systems lacked access controls to prevent deletions or alterations to raw data. For example, our investigator reviewed the electronic folder containing data files generated when your firm tested (b)(4) batches of (b)(4) API for residual solvents by gas chromatography (GC). The investigator compared the file names in the folder with the metadata generated by the Chemstation software you used to operate your GC system, and found that two chromatograms had been deleted from the system. Because there were no controls restricting operators’ or supervisors’ abilities to alter or manipulate the data, an analyst had completed two runs and deleted the results, and then changed the subsequent file names in the folder where reported data was stored to make it appear that the deleted runs never occurred. In your response, you stated that two injections were deleted from the system because the analyst believed that an unstable baseline made retaining the files unnecessary. You also confirmed that your software had no access controls and that your analysts had authorization to delete data.
Failure to have laboratory control records that include complete data derived from all laboratory tests conducted to ensure compliance with established specifications and standards. Your quality control laboratory failed to record and maintain complete data from analyses of your (b)(4) API. For example:

- Prior to conducting official analyses, your quality control laboratory performed “experimental” analyses on product batches to assess whether your API met specifications, but failed to document these “experimental” tests in official laboratory records or to justify their exclusion. Our investigator found the results of 2,404 high performance liquid chromatography (HPLC) injections in a folder titled “Experimental” on instrument SZG-002-006l. Your quality unit indicated that these “experimental” injections were being conducted in all (b)(4) chromatographic units in your quality control laboratory. Your management provided different explanations in an attempt to justify the practice, including “fear” that the sample results would not pass.

- Our review of the audit trails of chromatographic systems SZG-002-009, -010, -011, and -012 documented that your laboratory analysts deleted raw chromatographic data on multiple occasions. Your firm indicated that analysts may have been testing the system and may have deleted associated files. You also indicated that the deleted files may represent aborted analyses. However, we documented that some audit trail entries of deleted raw data files contained batch numbers for actual batch samples being tested. There is no assurance that laboratory records and raw data are accurate and valid.

- We acknowledge your decision to revise your current procedure for the testing of (b)(4). In response to this letter, provide a summary of how your chromatography procedures will conform to U.S. Pharmacopeia requirements, including those for the establishment of system suitability. In addition to deciding to revise your (b)(4) testing procedure, in your response you commit to acquiring additional chromatographic instruments, restricting certain chromatographic instruments to specific analyses, installing a new data control system, upgrading instrument software, and enabling data integrity features included in the laboratory software. Your response is inadequate. None of your explanations justify your failure to maintain complete records, nor do they support your practice of substituting repeat tests after failing results. Acquiring new instruments, installing new and upgraded software, and enabling various features on software are only effective if you have implemented appropriate procedures and systems to ensure that your quality unit reviews all production and control data and associated audit trails as part of the batch release process.
Health Authority Data Integrity Guidance Documents

- MHRA GMP Data Integrity Definitions and Guidance for Industry -March 2015 (Final)
- FDA Data Integrity and Compliance With CGMP Guidance for Industry Draft Guidance (18 Q&As) -April 2016 (Draft)
- WHO: Annex 5, Guidance on good data and record management practices -June 2016 (Final)
- MHRA GxP Data Integrity Definitions and Guidance for Industry Draft version for consultation –updated draft Guidance July 2016 (Draft)
- EMA (European Medicines Agency) (23 Q&As) –Aug. 2016 (Final)
- China -Drug Data Management Standard –October, 2016 (Draft)
- Parenteral Drug Association (PDA): Elements of a Code of Conduct for Data Integrity (2015 –Free on PDA Website)
## Comparison of Guidance Documents

<table>
<thead>
<tr>
<th>Guidance</th>
<th>Emphasis on using a risk-based approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>MHRA</td>
<td>Yes - The effort and resource applied to assure the validity and integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient or environment. When taken collectively these arrangements fulfill the concept of data governance.</td>
</tr>
<tr>
<td>WHO</td>
<td>Yes - The effort and resource assigned to data and record governance should be commensurate with the risk to product quality. The risk-based approach to record and data management should ensure that adequate resources are allocated and that control strategies for the assurance of the integrity of GxP data are commensurate their potential impact on product quality and patient safety and related decision-making.</td>
</tr>
<tr>
<td>EMA</td>
<td>Yes - The effort and resource assigned to data integrity measures should be commensurate with the risk to product quality, and balanced with other quality assurance resource demands.</td>
</tr>
<tr>
<td>FDA</td>
<td>Yes - FDA expects that data be reliable and accurate (see the “Background” section). CGMP regulations and guidance allow for flexible and risk-based strategies to prevent and detect data integrity issues.</td>
</tr>
<tr>
<td>PIC/S</td>
<td>Yes - The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality resource demands.</td>
</tr>
<tr>
<td>China</td>
<td>Yes - Relevant measures shall be taken according to the risks in data generation, record, storage, and use in the process of data management to ensure data integrity.</td>
</tr>
</tbody>
</table>
Possible Approaches to Data Integrity Governance

- Consider regulatory data integrity requirement in scope during requirements gathering phase

- As we progress during project phase perform assessment to see gaps and remediate gaps before go-live

- Assume Data Integrity Risks do not exist and do nothing
  - Highest Risk, Lowest Effort

- Zero Tolerance for Data Integrity Risks
  - Lowest Risk, Highest Effort
  - Not really achievable without diverting resources

- Risk-Based Approach
  - Best approach to allow focus on high risk opportunities
  - Based on documented risk assessment and remediation (if required)
Questions?
Case Study EU Annex-11 and MHRA

Case study MHRA

Case study EU annex 11
Questions?