Data Integrity
for the Microbiology Laboratory

Public

Agenda

- **Useful Sources of Information**
- **Define "DATA"**
- **ALCOA Principles**
- **Data Integrity Risks**
- **Regulatory Expectations**
- **Tools for Assessing Risk**

Disclaimer

- **These are my observations and suggestions.**
- **Nothing is black and white.**
- **There may be no correct or incorrect suggestions.**
- **There are pros and cons to everything**

Public

Useful Sources of Information

- Food and Drug Administration (FDA)
  - Data integrity and Compliance with cGMP Guidance for Industry, April 2016
- Europeans Medicines Agency
  - Data Integrity (Aug2016) Draft
- Medicines & Health Products Regulatory Agency (Jul2016) Draft
  - MHRA GxP Data Integrity Definitions and guidance for Industry
- Parenteral Drug Association (PDA)
  - Elements of a Code of Conduct for Data Integrity
- World Health organization (WHO) Annex 5
  - Guidance on good data and record management practices
- PDA Book Assuring Data Integrity for the Life Sciences
- Pharmaceutical Inspection Convention (PIC/S) Draft guidance 2016
  - Good Practices for Data Management in Regulated GMP/GDP Environments

Recent Publications

- Data Integrity Issues in Microbial Testing
  - Cheryl Platco and Anthony Cundell, authors
  - American Pharmaceutical Review, Sep/Oct2017
- Microbiological Test Data-Assuring Data Integrity
  - Edward Charles Tidswell & Tim Sandle, authors
  - PDA Journal of Science and Technology, 2017
- What is Data Integrity?
  - Anil K. Rattan, author
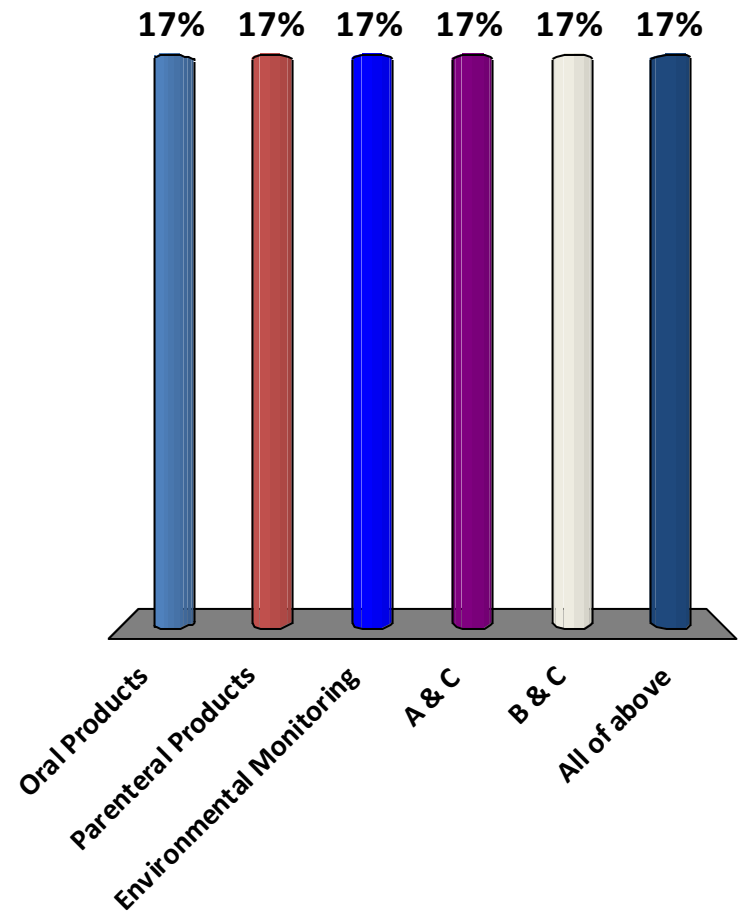 - PDA Journal of Science and Technology, 2017

Public

My laboratory tests samples for:

A. Pharma

B. Medical Devices

C. Cosmetics

D. All of the above

25% 25% 25% 25%

Pharma   Medical Devices   Cosmetics   All of the above
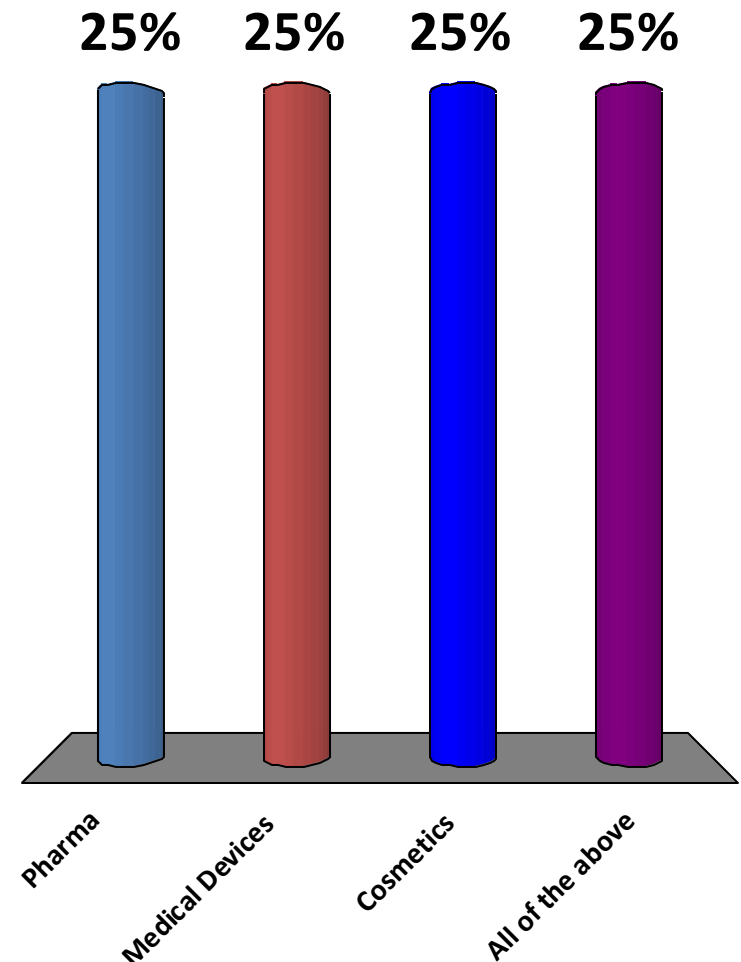
What types of samples you work with?

A. Oral Products

B. Parenteral Products

C. Environmental Monitoring

D. A & C

E. B & C

F. All of above

17% 17% 17% 17% 17% 17%

Oral Products | Parenteral Products | Environmental Monitoring | A & C | B & C | All of above

Public

I am familiar with ALCOA

A. True

B. False

50%   50%

True   False

Public

I am familiar with ALCOA +

A. True
B. False

50% **50%**
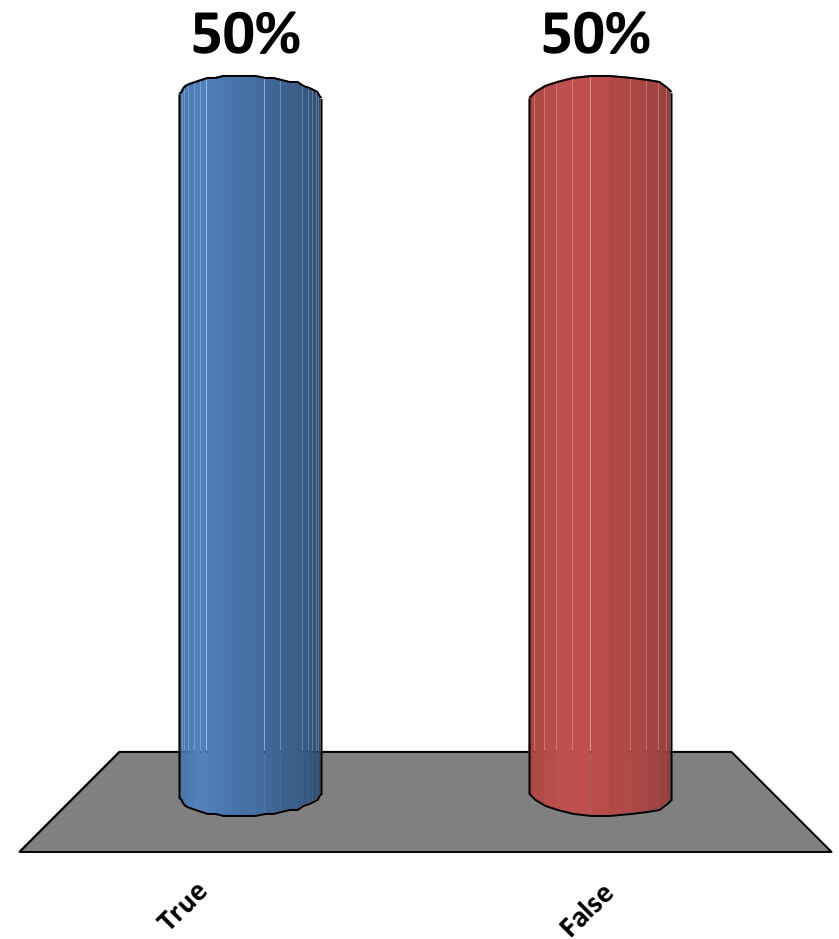
True False
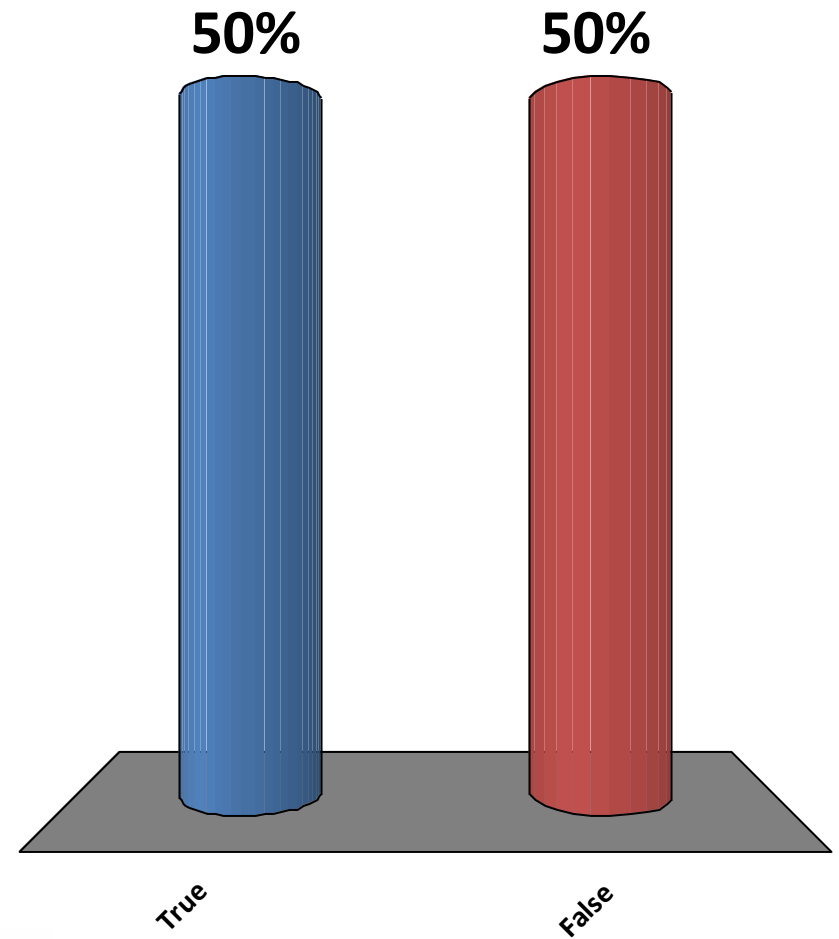
What is Data Integrity

- The extent to which ALL DATA ARE COMPLETE, CONSISTENT, AND ACCURATE.

- The data describe objective and factual status of all data values throughout the data lifecycle.

- ALCOA principles:
  - **A**ttributable: Traceable to a Unique Individual
  - **L**egible: Readable, Traceable Change, Permanent
  - **C**ontemporaneous: Activities Recorded at the Time they occur
  - **O**riginal: First Capture of the Data
  - **A**ccurate: Represents the actual conditions / data / information

ALCOA Plus (?)

- ALCOA Plus principles: Data are
  - **Enduring**
  - **Available**
  - **Accessible**
  - **Complete**
  - **Credible**

Public

Some Definitions

- **<u>Direct human observation of test result</u>**: Laboratory analyst views test outcome / result via direct observation and records the result via manual recording on laboratory raw data form or via direct entry into a system (example: GLIMS). No electronic capture or print out exist to independently verify the entry.

- **<u>Second Person Verification</u>**: A direct witness of a step to assure that the step was performed appropriately prior to commencing a subsequent step or an equivalent assurance.

- **<u>Second Person Check</u>**: A confirmation by a second person for accuracy at close proximity to the executed step and usually required before continuing with a subsequent processing step and/or GMP activity

- **<u>Second Person Review</u>**: A re-examination of the content of the data/record/report by a second person against raw data (where available) as an independent review in a timely manner to confirm document complies with ALCOA elements (attributable, legible, contemporaneous, original and accurate) and in compliance with current Good Documentation Practices, current GMP standards and established procedures. This includes the review of items that have not been second person Verified or Checked during a GMP activity and for which documented evidence is required to demonstrate compliance with instructions on which quality decisions are taken

Questions

- Is "data" also defined as reagent lot numbers, instrument #, etc.
- Does SSR have to confirm ancillary data accuracy?
- Does SSR have to view all objective interpretations of data (qualitative or quantitative?)
- Does all data have to be recorded one at a time or can data entry be batched specially if all "no growth" or "zero count"?
- How does one reconcile using electronic NB to capture real time execution of testing with aseptic technique?
- How granular (detailed) must signatures from all person involved in the operation be?
- Do we have to add more personnel to observe as second person where data interpretations are not electronic and are subject to interpretation.
- Do personnel have to have eye tests to prove they can see the detail which they are tasked for interpreting?

Let's Define "Data"

- **It is:**   **It is not:**

P **Public**
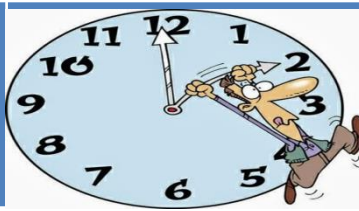
Attributable	Legible	Contemporaneous	Original	Accurate

Why the recent Interest

- Increasingly observed **violations in cGMP** for data integrity during inspections
- Resulted in warning letters, import alerts, consent decrees
    - Requirement that backup data are exact and complete, secure from alteration, inadvertent erasures or loss
    - Requirement that data be stored to prevent deterioration or loss
    - Requirement that activities be documented at the time of performance and lab controls are scientifically sound
    - Requirement that records be retained as original, true copies, or other accurate reproductions of original records
    - Requirement for complete information, complete data derived from all tests, complete record of all data, and complete record of all tests performed.

P Public

Microbiology Data Integrity Risks

- **High Risk**
    - **Analyst records incorrect data**
    - **No second opinion results for subjective interpretation of results**
    - **Analyst performs wrong method or wrong sample preparation**
    - **Missed critical data or incorrect information**
    - **Falsification or lack of authentic data due to uncontrolled lab worksheets**
- **Medium Risk**
    - **Real time data entry difficult**
    - **Incomplete data entries**
    - **Chain of custody for samples not real time.**
- **Low Risk**
    - **Improper recording of non-critical data**
    - **Real time entry of non-critical data (lot numbers, etc) not performed in timely manner**

Public

Regulatory expectations

- **Look for evidence of bad documentation practices**
  - Open drawers, look in trash bins or other locations for evidence of materials discarded.
  - Observe that there is no evidence of use of scrap paper, post it notes, writing on desks or transient paper
  - Observe that there is no evidence of discarded partially completed documentation of any kind
  - Assure that data is recorded and maintained for all preparations, solutions, etc.

- **Look for evidence of lack of electronic data integrity**
  - Technician/Lab Manager given ability to delete/alter files? Overwrite files? Change files?
  - Date / Time stamp on local equipment or network?

- **Look for good data retention practices**
  - Assure that records are original, maintained, and retrievable.
  - Assure that the retrieval process been challenged for misuse potential, and is retrieved data accurate and complete.

- **Look for misuse of documentation practices or fraud**
  - Look for uncompleted and discarded copies of data worksheets / notebooks.
  - Sheets should be pre-numbered and in chronological order.
  - Look for repetition of same data from run to run.

Attributable

- Data is linked to the person performing the action
  - Maintain a master signature and initial log
  - Only sign for the work you completed
  - Sign and date changes to documentation
  - Never leave work stations unattended
  - Use e-sigs when recording data/actions

Public

ATTRIBUTABLE

- Observation :

  While multiple employees participate in a process step that spans more than one shift, only the last person involved is required to sign the batch record for completion of the activity.

- Clearly ID who performed what.
  - How do we document teamwork?
  - How do we document multiple individuals working at performing at different times?
  - How do we document tasks over period of time?
- Paper records
  - In some ways easier than electronic
- Automated data trails: track data changes, repeats, or deletions.
  - Electronic systems can be copied, template, etc. for ease of use.
  - Time stamped
  - User may need to sign in and out repeatedly if teamwork is used to perform task.
  - do lab analysts,
  - operators, managers have "overwrite" or"delete" permissions?

Attributable

- **General Microbiology**
  - How do we control who executed the action, date, time for sample chain of custody, test setup, test execution, results reading, results reporting second person review /audit of data, data archival?
  - How granular are the critical steps? Are SOP's/methods not enough detail?
  - Do signature logs match GMP documentation signatures?
  - Are all employees involved in a step required to sign for the step?
  - Gate Records versus documentation – are employees signing for work checked into the site on the date / time that the work is purportedly completed?
  - Is data used in GMP processes or to make GMP decisions

- **Paper**
  - Is there a manual audit trail?
  - How are changes tracked? Revisions to documentation? Controlled copies of data result templates? Change control?
  - Do batch records and test records have space for initials or signature / date for significant steps?

- **Electronic**
  - Are we using electronic capture in Micro using automated equipment? If so, should have audit trail capability.
  - Is the audit trail "turned on"?
  - If an automated audit trail is not available, is a manual audit trail in place for
  - Who has the ability to turn audit trail on / off – and does it present a conflict of interest?
  - Does the automated equipment support unique userids / passwords?
  - Or, are shared userids / passwords used? (e.g. "system" appears as name)

Legible

- **Readable throughout lifecycle, permanent, identifiable changes**
  - **Use permanent ink**
  - **Write neatly**
  - **Follow established date and time format**
  - **No overwriting/scribbling of data**

Legible

- **Observations:**

  The investigator… observed the presence of opaque correction fluid in many of your production records…

  There are no procedures that address the use of signature stamps in lieu of handwritten signatures….

- **General**
  - **All data and meta data can be read, backup, stored and archived, with procedures for retrieval.**
  - **Resources/people to be a separate user, reviewer and administrator**
  - **Evidence of use of pencil or white out?**
  - **Are cross outs corrected with a single line, initialed and dated?**
  - **Are explanations provided if the cross out is not self evident (or completed well after the original entry?)**
- **Paper:** **Paper copy manual corrections must be signed, dated and explained.**
- **Electronic**
  - **Records in readable form, software programs that are necessary to read data need to archived and functional.**
  - **Users have unique ID and password.**
  - **Users should not have ability to overwrite or annotate or delete raw data.**
  - **Is critical data backed up on a frequency that minimizes risk of potential loss?**
  - **Where does backed up data reside and is it a secure location?**
  - **Look at order of events being performed – is data saved at appropriate times?**
  - **Are electronic signatures applied at appropriate times?**

Our testing data is captured in:

A. Paper records
B. Electronic records
C. Mix of electronic and paper records

33%   **33%**   **33%**

Paper records

Electronic records

Mix of electronic and paper …

Public
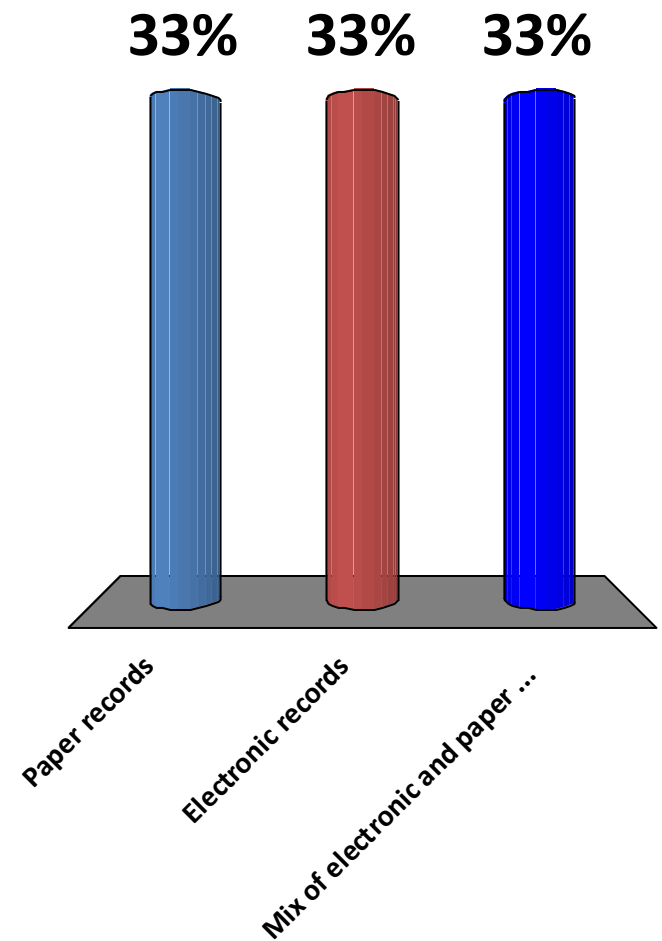
Contemporaneous

- **Activities recorded at the time they occur**

  - **Sign/date records at the time of activity completion**

  - **Never back-date or pre-date**

  - **Users must not have access to change date/time of electronic data**

Contemporaneous

- ## Observation:

    ….Specifically, an operator performed the in-process tablet (b)(4) testing for the (b)(4) mg tablet batch #(b)(4) without the batch record or a manufacturing form to document the results contemporaneously. …your operator stated that he records the two weights with (b)(4) significant figures into the batch record (located in another room) from memory.

- ## Data is recorded or entered when activity occurs.

    – **How do we maintain aseptic technique.**

    – **Do we document each step?**

    – **How granular must each step be?**

    – **Can we batch read/interpret data and then record batch?**

Public

Contemporaneous

- Are entries in logbooks in chronological order?

- Is their evidence of pre-populating GMP data. (electronic templating?)

- Is there evidence of complex numbers / calculations / GMP data being written on hands, scrap paper, workbench, or attempting to be memorized – and later transferred into the record?

- Review of batch records – does the timing of steps match up?

- Are there potentially two actions being performed by the same person at

- the same time? Is there a resource or manning issue?

- Is GMP documentation available at the point that the data is generated?

- How many system administrators are there for GMP systems, and do individuals responsible for the generation / approval of the data have the capability to change the time / date stamp?

Public

Original

- **Data as the file or format in which is was generated, preserving the integrity (accuracy, completeness, content and meaning) of the record**
    - **Retain all raw data and printouts**
    - **Original data must be recorded directly into GMP records**
    - **Original data must be reviewed**
    - **Electronic raw data files must be retained**
    - **Controlled in a manner which prevents unauthorized re-creation.**

Original

- **Observations**

  - Your firm repeatedly delayed, denied, limited an inspection or refused to permit the FDA inspection. An FDA investigator identified the presence of torn raw data records in the waste area and asked one of your firm's QA Officers to remove these torn raw data records for the investigator's review. This QA Officer presented the FDA investigator with approximately 20 paper records, none of which included raw data entries identified in the waste area earlier during the inspection. The FDA investigator then re-visited the waste area and found that the raw data records had been removed and placed in a different holding bag.

  -   ...claims that notebooks and datasheets are controlled. A pack of datasheets were observed in the laboratory that were not controlled. Analyst could use one, discard it and it couldn't be traced to that analyst.

  -   uncontrolled piece of paper with handwritten note related to analytical method and reagent being used was also discarded in the garbage bin.

  - No audit trail and no consistency checks had been implemented to prevent misuse of data.

Original

- **General**
  - **No sticky notes**
  - **No scrap papers**
  - **No plate lids???????**

- **Paper**
  - **Lab data sheets must be controlled so as not to be able to be discarded without explanation.**

- **Electronic**
  - **Includes all data, test results, sequence logs, metadata, audit trails**
  - **Must be able to recreate entire event**

Accurate

- Data represents the complete set of factual, actual data and meta data
  - Data must reflect the action/observation
  - All data must be controlled and retained for the lifecycle
  - Modifications to the data must be explained if not obvious
  - Meta data includes units of measure, method details, audit trail, date/time modifications

Accurate

Represents Who, What, Where, When, Why and How

- **Observation:**
    - The data for assay are generated by processing each result file individually using different processing parameters. The second person reviewer is not required to review each of the processing parameters used to generate results.
    - …only one operator was assigned to evaluate sterility test on the last day of the incubation period. To ensure reliability of the tests, your procedure needs to specify steps that enable objective evaluation, such as assigning two operators for evaluation on the last day.

- **General**
    - Complete set of factual, actual data, and metadata
    - There are examples of fabricated or fraudulent data.
    - Only those individuals responsible for completion of a step or activity are signing for the activity.
    - Data from previous batches cannot be copied / renamed for current data
    - All data generated for a sample is made visible and considered in the decision.
    - Non-conforming results must be formally investigated, and a root cause identified to enable the results to be invalidated.

Accurate

- **Paper**
  - **All steps and activities are recorded in sufficient detail to recreate the data picture.**
  - **All calculations are checked for accuracy.**
  - **All steps are recorded in a logical order.**
  - **Worksheets and Notebooks must be controlled. There should be a mechanism to control the issuance of the worksheets / notebooks to analysts, and reconciliation of worksheets used versus returned / destroyed. Sheets should be pre-numbered in chronological order, or have a similar process to ensure.**
  - **The copy of a worksheet should be distinguishable from the original worksheet.**

- **Electronic**
  - **Are instrument logs available, and do the physical entries match the electronic system entries?**
  - **All electronic calculations are validated for accuracy.**
  - **Ensuring laboratory analyst / managers are not granted access to delete, overwrite, copy, alter, annotate or otherwise manipulate data (unless permitted per the method and tracked via audit trail).**

5 Why's Tool

- Determines cause and effect relationship of problems.

- Used to determine the root cause of problem.

- Adapt for assessing risk of DI breaches.
  - Ask Why? 5 times or more to drill to root of problem
  - Ask Who, Where, What When and Why as it applies to each question.

FMEA tool for Risk Assessment
Failure Mode and Effects Analysis

Process Step	Key Process Input	Potential Failure Mode	Potential Failure Effects	S E V	C L
What is the process step?	What are the Key Process Inputs? (KPIV's)	In what ways can Key Inputs go wrong? (Process fail to meet requirements)	What is the impact on the Key Output Variables (customer requirements) or internal requirements?	How Severe is effect to the customer?	Classify Critical characteristics*

1. List of Design Functions or Process Steps
2. Select the KPIV to be studied.
3. Identify the possible failure modes (there may be several). Brainstorm and experience based!
4. Determine the effect of each failure mode.
5. Rate the severity of the failure.
6. What is the CTX?

th

14

FMEA Severity Rating
adapted for microbiology QC testing
(suggestions!)

1   Product quality not affected or insignificant
2   Product quality not affected, unlikely to be noticed.
3   Product quality not affected, and does not cause patient harm.
4   Product quality may be affected, does not cause patient harm, but may reduce product quality
5   Product quality may be affected, potential to cause minor patient annoyance, but may cause noticeable product quality attribute issues.
6   Product quality affected, potential to cause minor patient annoyance, complaints may be filed.
7   Product quality affected, complaints are likely, patient harm or dissatisfaction may occur.
8   Product quality compromised, complaints and recalls likely occur, patient safety issues occur with minor affects due to contamination or spoilage.
9   Product quality compromised, complaints and recalls occur, patient safety issues occur with moderate affects due to contamination or spoilage.
10 Product quality severely compromised, spoilage and contamination visible, and/or patient affects significant.

FMEA Risk Assessment continues

Potential Causes	O C C	Current Process Controls	D E T	R P N
What causes the Key Input to go wrong? (How could the failure mode occur?)	How frequent is cause likely to occur?	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	How probable is Detection of cause?	Risk Priority # to rank order concerns

FMEA OCCURRENCE RATINGS

1	Likelihood of occurrence is remote
2	Low failure rate with supporting documentation
3	Low failure rate without supporting documentation
4	Occasional failures
5	Relatively moderate failure rate with supporting documentation
6	Moderate failure rate without supporting documentation
7	Relatively high failure rate with supporting documentation
8	High failure rate without supporting documentation
9	Failure is almost certain based on warranty data or significant testing
10	Assured of failure based on warranty data or significant testing

7. List the cause of each failure (there may be several). Brainstorm and experience based!
8. Rate the failure frequency of occurrence.
9. Identify the current controls to prevent the failure from occurring.
10. Rate the ability to detect the failure once it occurs.
11. Calculate risk priority number: Sev*Occ*Det - a scale of 1 to 1000.

Public

FMEA continues

FMEA DETECTION RATINGS

1   Certain that the potential failure will be found or prevented before reaching the next customer

2   Almost certain that the potential failure will be found or prevented before reaching the next customer

3   Low likelihood that the potential failure will reach the next customer undetected

4   Controls may detect or prevent the potential failure from reaching the next customer

     Moderate likelihood that the potential failure will reach the next customer

     Controls are unlikely to detect or prevent the potential failure from reaching the next customer

     Poor likelihood that the potential failure will be detected or prevented before reaching the next customer

8   Very poor likelihood that the potential failure will be detected or prevented before reaching the next customer

9   Current controls probably will not even detect the potential failure

10   Absolute certainty that the current controls will not detect the potential failure

FMEA completion

Actions Recommended	Resp.& Target Date	Actions Taken	S E V	O C C	D E T	R P N
What are the actions for reducing the Occurrence of the cause, or improving Detection? Should have actions on high RPN's or Severity of 9 or 10.	Who's Responsible for the recommended action? What date?	What were the actions implemented? Include completion month/year. (Then recalculate resulting RPN.)				

12. Documents actions recommended based upon RPN pareto. These are generally short term containment activities.
13. Identifies responsibilities and timeline.
14. Documents actual actions taken
15 – 18. FMEA scores on revised process.