Q O R M

Quality Operations Regulatory Management

Common Sense. Compliance. Delivered.

# Data Integrity –
# Is your Company at Risk?

# Introduction

# Compliance Hot Button – Data Integrity

- Data Integrity has been a focal point for regulators on a global basis
  - **FDA September 1991: Application Integrity Policy – Fraud, Untrue Statements of Material Facts, Bribery, and Illegal Gratuities**
    - Five companies on CDER list – ONE from India, FOUR from USA
  - MHRA Guidance March 2015: GMP Data Integrity Definitions and Guidance for Industry
  - WHO Guidance September 2015: Good Data and Record Management Practices
  - FDA Guidance for Industry April 2016: Data Integrity and Compliance With CGMP
    - 21 out of 28 FDA Warning Letters involved Data Integrity in 1st half of 2015
  - PICS August 2016: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments
  - EMA Questions & Answers August 2016

# Definitions

- Data
  - Data is the record of a transaction (recording the transaction of data, is data in itself)
- Data Integrity
  - The extent to which all data are complete, consistent and accurate throughout the data lifecycle.
- Data Lifecycle
  - Period of time from moment data is recorded to the end of the archiving.
- Good Documentation Practice
  - Standard describing the creation and maintenance of documents and records.
- Application Integrity Policy
  - FDA's approach regarding the review of applications that may be affected by wrongful acts that raise significant questions regarding data reliability.
- Information
  - Data, packaged and processed and sent into a direction with the intent to influence decision making

# Importance of Data Management

- Assures the quality, safety and efficacy of the drugs
- The documented data is the only record of the activity presenting the quality of the product
- Reliance on the data presented
- Questioning Data Integrity = Loss of Trust
- Recent FDA Hot Topic
  - "Guilty until Proven Innocent"
- Submitting false data to the FDA is a criminal violation under FD&C Act (CGMP /adulteration provisions)

# Data and Application Integrity

- All records submitted to FDA & supporting documents in the possession of the applicant are accurate & true representations of:
  - Actual tests performed & the actual test results
  - Actual manufacturing & quality control steps & procedures associated with the development and manufacture of the submission batch (clinical/pilot or bioequivalence) and commercial operations
  - Any other actions and conditions associated with the application

- Absence of a **pattern of unexplainable discrepancies** between data in records submitted to the FDA and data in the original records maintained by the applicant.

# Application Integrity Policy (AIP)

- An “administrative action”
- Once AIP is invoked, FDA suspends review of the application or applications until the provisions of the AIP are met by the applicant holder.
- Intended to assure the accuracy and reliability of data & information in applications submitted to FDA for scientific review and approval.
- No statute of limitations.

# Data Management – Only a Quality Control Issue?

NOT REALLY!

- See the following recent examples from FDA warning letters

# Warning Letter 1

***“Your firm failed to follow written procedures for production and process control designed to assure that the drug products you manufacture have the identity, strength, quality, and purity they purport or are represented to possess, and to document same at the time of performance (21 CFR 211.100(b)).***

At your Chikalthana site, our investigators observed poor documentation practices during in-process testing. 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.

The FDA investigator was informed that the pre-test and post-test weight values are documented in the batch record located in a separate manufacturing room rather than in the same room where the actual weights are measured. Moreover, your operator stated that he records the two weights with (b)(4) significant figures into the batch record from memory.

Your investigation into this issue is inadequate because it did not consider other in process tests or whether the operator(s) have been involved in the same poor documentation practices for others batches. Your response does not indicate whether this poor documentation practice is an isolated case or is a matter of widespread behavior in this facility.”

# Warning Letter 2

“On March 19, 2013, an FDA investigator interviewed the Production Head regarding his knowledge of the unofficial batch record forms being used to record the results for the visual inspection of drug products. The Production Head stated that he had only seen this unofficial defect data for "1 to 2 batches". The FDA investigator had an earlier conversation with two manufacturing operators, who stated that the Production Head had directed this practice throughout the manufacturing facility and regularly requested and reviewed the unofficial BMR visual inspection results.

On March 21, 2013, the Production Head stated that he was fully aware of the practice of using unofficial batch record copies during the course of manufacturing operations. The Production Head acknowledged that he had provided inaccurate information in the previous instances. By stating that the data that existed was limited to one or two batches and that no other data existed, you provided some, but not all, of the records requested by the investigator that FDA had the authority to inspect.

Additionally, you limited access to or copying of records for the FDA inspection. Because you denied the existence of records that FDA had requested and had the authority to inspect in order to obstruct the direct observation of the requested documents, you delayed the inspection.”

# Warning Letter 3

***"Failure to document production and analytical testing activities at the time they are performed.***

During our inspection, we found that test results and other entries in the production records were not entered while batches were in production.  For example,

a.    The investigator observed **(b)(4)** batch **(b)(4)** production on March 18, 2014. The start and stop times and **(b)(4)** for Step #**(b)(4)** were not recorded or signed in the batch record contemporaneously.

b.    For your **(b)(4)** products returned due to the presence of extraneous threads, the investigator found many inconsistencies in your reprocessing batch records.  Specifically, operators signed batch records for periods when they were not in your facility, indicating these activities were documented by personnel who did not perform them.  During the inspection, and in your written responses, your managers admitted that the batch records were created after the manufacturing process."

# Shades of Grey

| Innocent Ignorance | Surprising Sloppiness | Malicious Malfeasance |
|---|---|---|
| Misconduct of uninformed kind | Misconduct of lazy kind | Misconduct of sleazy kind |
| Act is unintentional;<br>Non-Compliance is unintentional | Act may or may not be intentional;<br>Non-compliance is unintentional | Act is intentional;<br>Non-compliance is intentional |
| Discarding source documents after accurate transcription;<br>Deleting e-files after printing | Inaction, inattention to detail, inadequate staff, lack of supervision | Data manipulation, data falsification, mis-representation, with holding critical information |

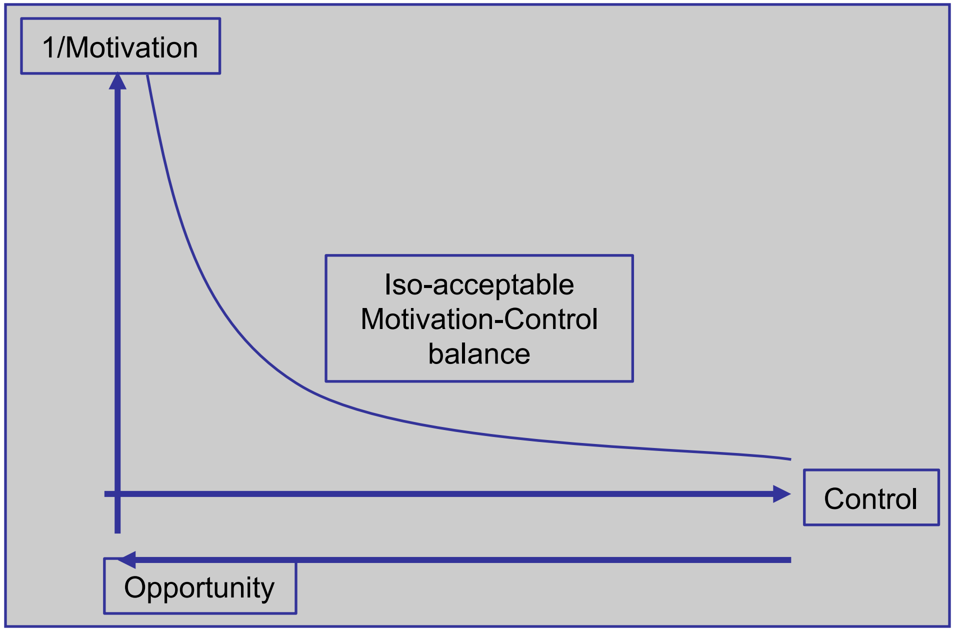
**Misconduct does not include honest error or honest difference of opinion.**

# Good Documentation Practice

- **A**ttributable
  - Identifying the person generating the data
- **L**egible and Permanent
  - Can be read by another person and cannot be erased or altered
  - **Permanent → Data Life Cycle**
- **C**ontemporaneous
  - Recorded at the time of activity
- **O**riginal Record
  - "Raw Data"
- **A**ccurate
  - Exact and True

# Prevention

# Data Integrity – Regulators focus on the motivation/control framework



**Motivators**

- Operational inefficiencies
- Pressure to succeed
- Too many review cycles (someone else will catch my mistake)
- Lack of training
- Unstable, not well understood processes
- Too many unknown failure modes of process

**Control Failures**

- Unclear or inefficient procedures regarding data integrity and/or review
- Lack of control over forms and / or sample
- Controls not forcing accountability
- Disjointed electronic systems
- Too many transcription steps

# Data Integrity – Motivation/control takeaway

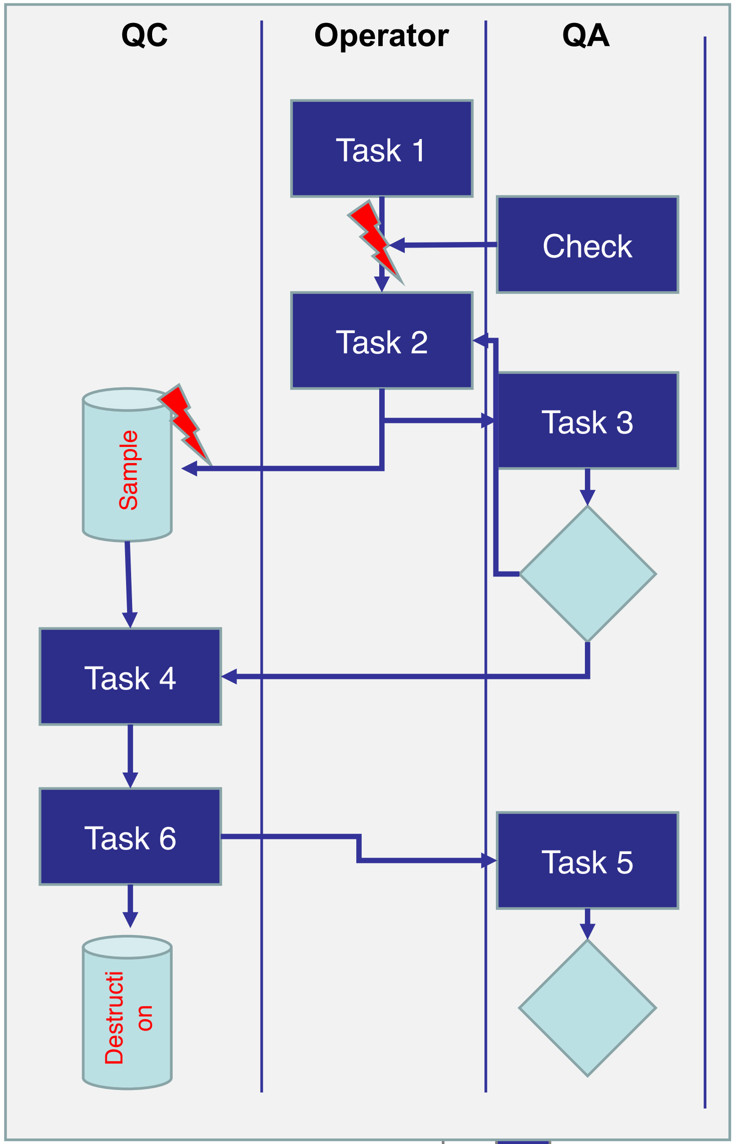
- If the motivation is high enough, no level of control will be sufficient

- Too many controls, in particular incongruent controls, may themselves be drivers for higher motivation for untoward data manipulation
  - Too many review cycles lead to the belief that someone else will find whatever was wrong
  - Many review cycles may slow down work and increase performance pressure
  - Continuous context change between execution and review may impede on concentration to get a good job done

- Well understood processes lead to fewer issues, including DI issues
  - Understand risks in processes
  - Understand "benign" diversions and plan for them

# How to determine whether your organization has DI risks?
# AKA : DI Stress Test

| | |
|---|---|
| **Control** | - **Start with understanding the workflow**<br>- **Individual tasks**<br>  - **Validated and failure modes understood?**<br>  - **Are there unspecified "benign" failure modes?**<br>- **Determine the controls for the individual tasks**<br>  - **Are tools DI breach proof?**<br>  - **Are there places to hide?**<br>  - **If yes, issue remains in transfers of data**<br>- **Tools**<br>  - **Are tools and job aids helping to be successful?**<br>- **Determine whether control efforts increase DI value**<br>  - **Avoid repetitive, non-value add review cycles**<br>  - **Lean, not mean review** |
| **Motivation** | - **Personnel suitability**<br>- **Sufficient personnel for planned throughput?**<br>- **Sufficient space and tools for planned throughput?**<br>- **Technical expertise?**<br>- **Mutual respect and understanding of roles and responsibilities** |



# How to determine whether your supplier has significant DI risk

- When auditing a supplier you may not have the time to go in-depth as in your own organization
- The Motivation/Control framework is a good starting point to determine where risk factors lie
- An approach more aggressive than usually found in an audit and more akin to an inspection may be called for
- Many good ideas have been published that help discover control failures or motivators for untoward DI behavior:
  - If so, are there accommodations for such weaknesses in the SOPs?
  - How much time do analysts, QA people, leaders, etc., spend with review vs. practical work?
  - How many review cycles exist?
  - Is there a full loop to control documents, protocols
  - Are systems Part 11 compliant
  - Determine level of deviations: Too many deviations may look like lack of focus, but too few deviations is suspicious. What is the backlog?
  - Others

# Stress Test Cheat Sheet

## Motivation

  - Truth: No analyst/operator gets up in the morning to cheat at work
  - Truth: Most DI breaches are discovered because analysts/operators are telling you about it

- ➔ Engage with analysts away from supervisors to gage workload and pressure
  - Clarify that you are not out to get him or her
  - Clarify that you respect that he/she is just as interested in data integrity as you are
- Do analysts know of weaknesses in process or methods?
- Is the unit staffed for planned throughput? (Check backlogs)
- Is the environment suited for planned throughput?
- Is there space for review activities at planned throughput? (Paper review takes space)
- Does training elaborate which data and meta data are critical to be conserved?
- Are processes stable? (Check deviations)
- Are process weaknesses understood and controls in place? (Check **repeat** deviations and CAPA)
- Are there repetitive review cycles? (Someone-else-catch it mentality)
- Is there a lot of review of things that "can't go wrong"? (Boredom)

# Stress Test Cheat Sheet

## Controls

- **Determine change of control steps in workflow (Can things fall through the cracks?)**
- **Determine whether controls around these changes are adequate (How would you find what fell through the cracks)**
- Does QA have technical competency? (How obtained?)
- Is access to instruments well controlled? (no off-the-books measurements)
- Is issuance and return of forms well controlled? (logbooks, registers, LIMS)
    - What is the review frequency for logbooks and registers?
- Are samples well controlled (until destruction)?
- Are electronic systems well controlled and validated?
    - This includes printouts
- Are electronic systems trained on finding inconsistencies and perform verification steps?
    - Controlled vocabulary
    - Alerts if values are left blank
    - In-machine calculations vs. Excel calculations

# Stress Test Cheat Sheet

## Tools – Job Aids

- Are worksheets or batch records structured to facilitate correct data entry
- Is the environment setup to allow concomitant data entry?
  - Space?
  - Availability of batch record?
- Are procedures “feasible”?
  - If people use workarounds the procedure is NOT feasible
- Are “allowable” diversions from main process parameters well explained and discriminated from non-allowable
- Are there tools to record review observations and their resolution?
- Are there mechanisms/tools to provide management feedback about review observations, even if they don’t lead to the level of deviations/investigations?
- Is there a continuous improvement mentality with respect to tools?

# Remediation

# Remediation after Discovery of Data Integrity

- If issue has been discovered by company, notify FDA and include in remediation
  - Potential Field Alert Situation

- **<u>All trust</u>** in company and its supplied data has been lost

- **<u>DO NOT ATTEMPT TO FIX YOURSELF</u>**

- Trust needs to be regained with the FDA and customers

# Remediation after Discovery of Data Integrity, continued

- Trust has to be regained through
  - Review and remediation by **<u>independent</u>** entity
    - Develop protocol to address the interim controls
  - Implementation of interim controls:
    - Investigation into **<u>true</u>** root causes
      - Implementation of adequate CAPAs
      - **<u>NO TESTING UNTIL CAPAs ARE IMPLEMENTED</u>**
      - Effectiveness checks → End point of Remediation Activities
    - Determine process for Handling DI Issues discovered during review.
    - **<u>Prospectively</u>** all data to be certified by third party
    - **<u>Retrospectively</u>** certification of data by third party

# Interim Controls

- **<u>Prospectively</u>** all data to be certified by third party
  - All data (stability and release) after testing commences again
- **<u>Retrospectively</u>** certification of data by third party
  - Define scope based on expiry dates of products
  - Define priority of data to be reviewed based on risk to patient and review of complaint data
  - Define process for potential field alerts and recalls
  - Develop protocol and gain agreement by FDA
- DO NOT FORGET STABILITY DATA

# Data Integrity – After the 483

- The FDA will often require you to determine
  - To what extent data manipulation techniques (and which ones) were used
  - What is the amount of suppressed unfavorable data

- Forensic DI analysis can accelerate this process
  - Forensic DI can surface data integrity issues on a quantitative level
  - Forensic DI can alleviate concerns about usability of data

- **Here is what not to do**
  - A first instinct would be to try to analyze audit trails
  - Audit trails are not suitable for this task
  - **DO NOT ATTEMPT A FORMAL ANALYSIS OF AUDIT TRAILS.**
  - You will create too many false positives and then you have two problems
    - Answer the FDA and explain all the false positives

# Data Integrity – Forensic Auditing Can Detect DI Breaches

- Situation:
  - Company has fallen under suspicion to use free access to system's clock of GC machines to "re-measure" unfavorable data points
  - The company performed daily copies of data, unfortunately a lot of meta data in these copies got lost (so not a true backup)
  - Unfortunately, a recent true copy of the data has been lost due to a computer crash
- Task:
  - Determine whether on a routine basis the systems clock has been reset to allow overwriting of unfavorable data
- Scenario:
  - Analyst found it necessary to re-perform an experiment and set the time back to when original experiment was done. However, it is almost impossible to get minutes and seconds exactly right.
- Approach:
  - Put subsequent daily copies for ½ year for one instrument on a stand-alone computer
  - Wrote PowerShell script to read the first line of one of the meta files for each experiment. That file contained the actual time stamp of when the data was obtained
- Hypothesis:
  - The time stamp should not change from one day to the next for the same data point
- Result
  - Found several dozens of data points where exact time stamp differed by several seconds or minutes, indicating overwriting of data

# Data Integrity – Forensic Auditing Can Alleviate Concerns over DI Breaches

- Situation:
  - A company had no discernable technical or procedural controls that would guarantee data integrity
  - Analysts had taken upon themselves to develop “conventions” to secure data integrity
  - However, in one documented instance, it was observed that an analyst moved forward the workflow in LIMS outside the LIMS software (directly using SQL statement)
  - Upon FDA inspection, the company received a 483 with the request to clarify whether any of the data was still useful
- Task:
  - Determine whether lack of procedural and technical controls has led to breaches in data integrity
- Scenario:
  - Analyst may have deleted, overwritten, or simply walked away from unfavorable data
- Approach:
  - Analyze +13,000 data points
  - Scour systems tables, audit logs, backups for hints of data deletions, duplication of Analytical Requests, duplication of lot numbers
  - Consistency checks between meta data of eDC software and LIMS
- Result
  - A few minor inconsistencies were found that could be explained after examining in detail the worksheets

# Recap

- Data Integrity is not a new issue
- Data Integrity happens everywhere
- Be proactive
  - Don’t drink the Kool-Aid
  - Data Integrity Policy and Good Documentation Practice
  - Independent Audits
  - Ethics and Compliance Hot Line
- Once discovered take decisive action
  - Independent Third Party Review
  - Smart Interim Controls and Effective Review
  - Be open with the FDA, other Regulatory Agencies, and Customers

# Questions?

Dr. Thomas Thuene
Partner at QORM, LLC
tthuene@qormllc.com

Dr. Roland Bizanek
Strategic Partner at QORM, LLC
rbizanek@qormllc.com