Annual Meeting 2015
Philadelphia, PA

New Paradigms for
Manufacturing Excellence

Forensic Auditing for Data Integrity

Rebecca A. Brewer
Quality Executive Partners

QxP | QUALITY EXECUTIVE PARTNERS

Forensics

"the science of gathering and analyzing evidence to establish facts"

-wiseGeek.com

Forensic Accounting

Forensic Psychiatry

Why Use a Forensic Approach?

This approach focuses time and efforts on areas that should data integrity breaches exist, they would be most likely to be found.

Look for both:

- intentional breaches
- unintentional breaches

All Breaches are Governed by Motivation & Opportunity

Motivation is influenced by culture, current themes, programs, agendas, etc.

Opportunity is limited by controls and monitored by vigilant oversight

Understanding Motivation

Actions speak stronger than words!

Demonstrate your commitment:

- Leadership
- Programs
- Education
- Incentives
- Rewards
- Recognition
- Reprimands

Understanding Opportunity

What you say….
"N.O."

What they hear….
Next Opportunity

Opportunities are simply gaps in:

- Organizational Controls
- Physical Controls
- Document Controls
- Computer Controls
- QCU Oversight
- Vigilance
- Education

Forensic Auditors

- Qualified and skilled in data detail and tracing
- Independent
- Credible

Auditors need to remember this is not a typical GMP audit!

Forensic Audit Basics

Readying for the Audit:

- Identify the "crime"
- Identify the possible "crime scenes"
- Identify the potential "perpetrators" (the "perps")

Data Collection

- Secure the "crime scene"
- Investigate / interview the "perps"

Build Your Case and Write Your Report

- Analyze the collected data
- Identify the gaps and the needed CAPA
- Close the case file!

Identify the "Crime"

Just a few examples

Intentional Breaches

- Falsified Data
- Reprocessed Data without controls
- Operating outside of validation or registration parameters

Unintentional Breaches

- Unsecured systems
- Lack of Audit Trails
- Broken Security
- Unprocessed Data
- People not knowing any better*

* Perhaps the most common and most invasive type of data integrity failures…. EDUCATE!

Identify the Possible "Crime Scenes"

- QC Laboratories
- Process Control Systems and SCADA
- Batch Records
- Validation Records
- Regulatory Filings

Identifying the "Perps"

- Inventory your data systems:
  - Networked systems
  - Stand alone systems
  - Independent instruments
- Inventory your documentation systems
- Identify users and activities that are typically performed for the designated systems

Secure the "Crime Scene"

- Make an Audit Plan
  - What crime(s) [breaches] will be looked for?
  - What crime scenes [functions] will be targeted?
  - What perps [systems] will be audited?
- Identify needed Resources to "secure the scene"
  - What auditor skills are needed?
  - What support staff / specialists / system administrators are required?
  - What area personnel will be interviewed or will host the audit?
- Don't forget your crime scene "kit" – be prepared for photographs, screen shots, downloads and printing

Investigate

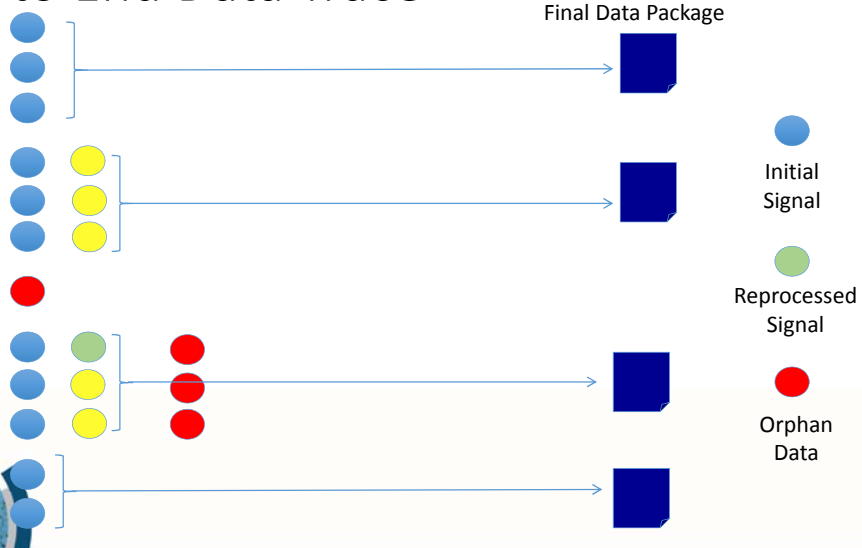
- Start at the beginning:
  - Begin with the point of data creation
  - Conduct an "End to End" Data Trace

    Process: Identify and review all data within a defined period of time to assess the ultimate end state of each and every signal acquired

    Objective: Ensure that no signals were acquired and overwritten, deleted, abandoned, or other wise not processed through to a final data report (i.e., Orphan Data)

    Scope: Select a time period that would reasonably allow for identification should they exist across data types (i.e., for laboratory consider instruments, analysts, methods, ultimate use of data, and any other relevant factors such as market)
  - Follow the data through each stage of storage and transformation

End to End Data Trace



Investigate (continued)

- At each stage look for:
  - Who has access?
  - Where is the audit trail? Is the audit trail accurate?
  - How is the data transformed? Is the transformation performed following validated procedures?
  - Is the data handling and transformation covered by SOP(s)?
  - When is the data reviewed and approved?
  - Where / how is the data stored and/or archived?

Investigate (continued)

- Interview personnel:
  - Ask what procedures are followed
  - Ask individuals of different roles and responsibilities to demonstrate their access and their typical actions
  - Witness routine data interactions including creation, transformation, storage, review, approval and archival
- Review Compliance with:
  - Validation parameters
  - Regulatory filings
  - 21 CFR Part 11 requirements

"The Clues" (a laboratory example)

- Where to look: Opportunity rich environments
  (e.g., is there a method with a high number of deviations, OOS or change controls that might indicate a lack of control that might tempt personnel to "cheat the system"?)
- What to look for:
  - Does the audit trail match the data that is under review?
  - Do you see clear traceability in the injection sequence numbers?
  - Do you see reprocessing, retesting or resampling? Approvals? Causes?
  - Evidence of pre-injections or cherry-picking of standards and run controls?

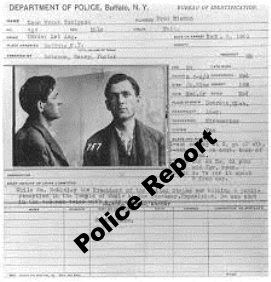
"The Clues" (continued)

- Do we see technical problems routinely with our runs?
  (e.g., runs cut short, differences in integration parameters, samples run with different times)
- What does the culture in the lab tell us?
  (e.g., rewards for low OOS rates, pressures on release timing)
- What do our investigations tell us about our culture?
  (e.g., over-use of most probable root cause, focus on use of retest)

Etc., etc., etc.

Analyze the Collected Data & Assess Gaps

- Collect:
  - Screen shots
  - Data files
  - Photographs
  - Printouts
- Organize the gap types:
  - Intentional breaches
  - Unintentional breaches due to failures in:
    - Inadequate physical or electronic security or access controls
    - Faulty or weak procedures
    - Missing compliance elements
    - Gaps in oversight



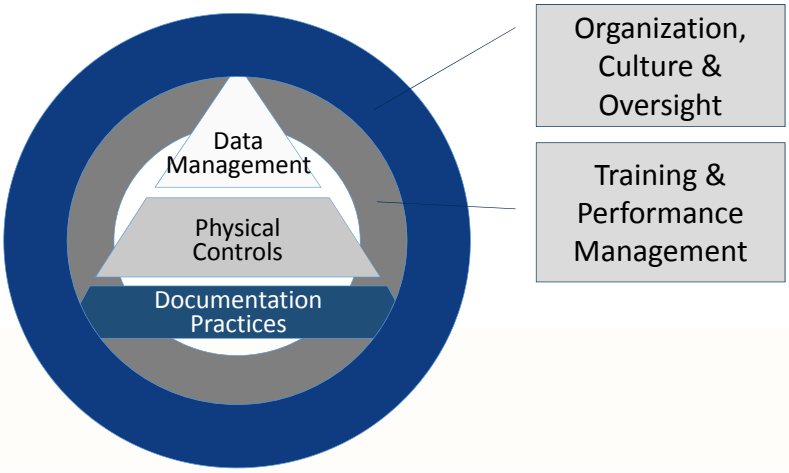
Identify CAPA

- Effective CAPA ensure holistic corrective actions
- Review planned CAPA across all stages of data acquisition, transformation, approval, storage and archival to ensure adequacy
- Consider planned CAPA from the perspective of different organizational roles to ensure integrity of the solution
- Verify that CAPA includes solutions that encompass:
  - Physical security
  - Electronic security and traceability
  - Administrative and procedural controls
  - Training and awareness

Continuing Vigilance

- Periodic Reviews for Orphan Data
- Data and Application Integrity Audits
- Consider the use of advanced forensic techniques (e.g., use of statistics and/or programs to identify patterns, data too good to be true)
- Management Controls
- Front Line Supervision
- Metrics – Monitoring and ACTION!
- Training and Education at all levels!

Data Integrity Controls
Opportunities for Technology Improvements



The Needle in the Haystack

Absence of evidence is NOT evidence of absence!

"If the only evidence for something's existence is a lack of evidence for it not existing, then the default position is one of skepticism and not credulity."

-rationalwiki.org

Questions?

Presented by: Rebecca A. Brewer
Quality Executive Partners
bbrewer@qualityexecutivepartners.com