VTI LIFE SCIENCES

nqa. ISO 9001 Registered

Parental Drug Association Validation Symposium

Preparation for Data Integrity Based Inspections

October 11, 2018

William Honeck, VP West Coast Operations

Introduction

- **WILLIAM HONECK** is the Vice President of West Coast Operations for VTI Life Sciences, Inc. He has over 25 years of experience in the pharmaceutical, biotechnology, and medical device industries. Prior to joining VTI Mr. Honeck held senior level positions within the industry including Associate Director positions within Validation, IT, and QA at Gilead Sciences, Johnson and Johnson, and Scios. He received a BSc Degree in Biochemistry from University of California, Davis.

- Mr. Honeck has led numerous validation projects while serving in Analytical Development, Quality Control, IT, and Quality Assurance capacities. His expertise includes establishment of Quality Systems and validation project management, development of Validation Master Plans, validation SOPs, risk assessments, and qualification protocols for computerized systems, utilities, equipment, and analytical instruments with a focus on data integrity. In addition, he has served as an SME in numerous Regulatory Agency Inspections.

- He can be contacted by email: william.honeck@validation.org

Agenda

- Part 1 – Prepare for a Data Integrity Inspection
  - History of DI related regulations and guidances
  - Warning Letter trends
  - Key Definitions
  - Policies & SOPs
  - Creation of data flow diagrams
  - Auditors’ expectations
  - Preparation of SMEs

Agenda

- Part 2 – Management of Investigators During the Inspection
  - Preparation for the instrument/system walk-through
  - Good practices for SMEs
  - Managing findings, prioritizing and implementing CAPAs
  - Overview of common findings/issues
- Knowledge Exchange Session
  - Share DI based audits/inspection experiences

History of CSV/DI Related Regulations & Guidances

- 21 CFR Part 211.68 Automatic, Mechanical, & Electronic Equipment – Sept 1978

- 21 CFR Part 11 Electronic Records and Electronic Signatures – March 1997

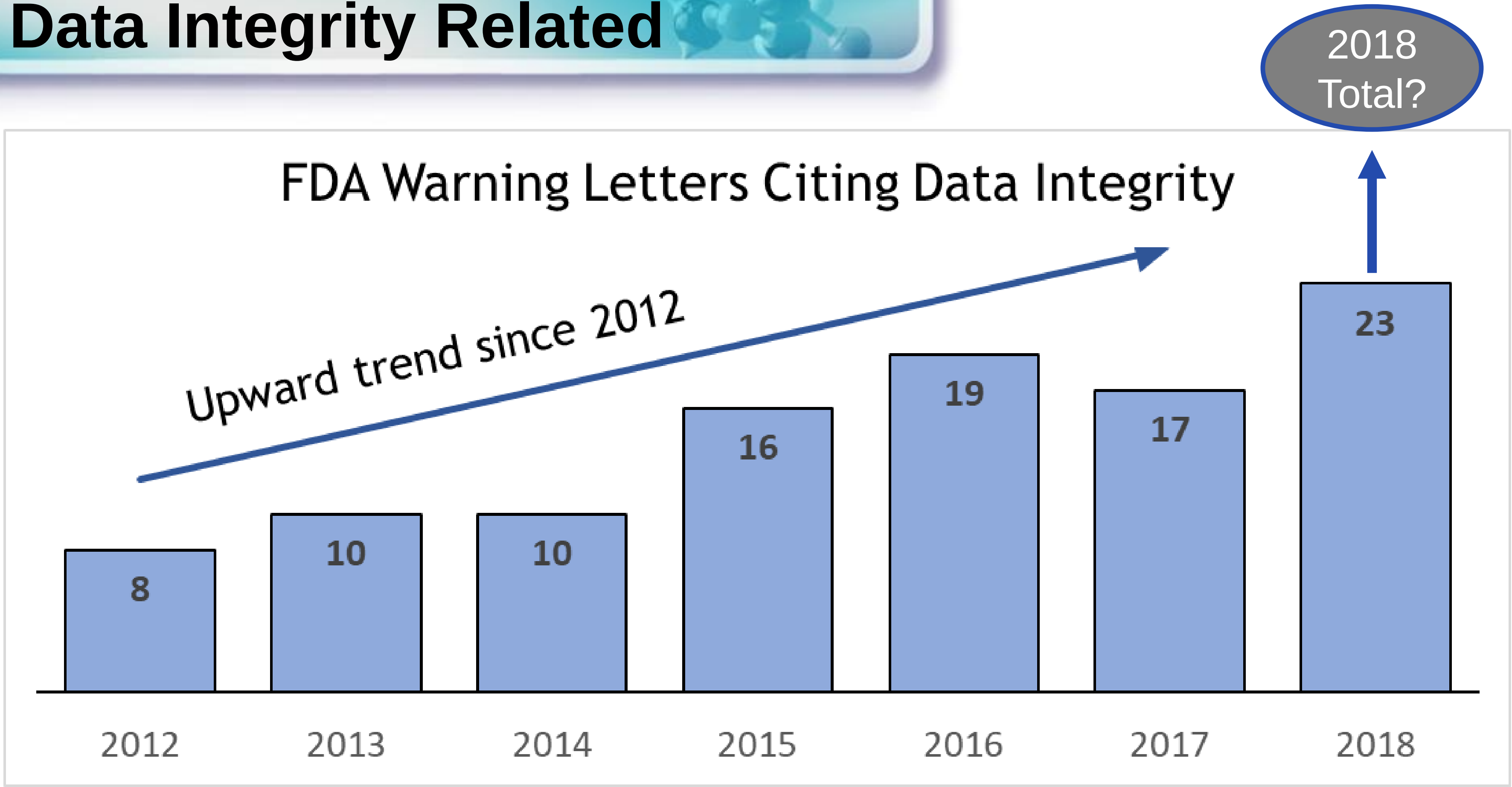
- EudraLex Vol. 4 GMP, Annex 11: Computerised Systems - Jun 2011

- MHRA ‘GXP’ Data Integrity Guidance and Definitions - March 2018

- FDA Data Integrity and Compliance with CGMP, Draft Guidance – April 2016

(212.110(b), 211.100, 211.160, 211.180, 211.188, 211.194, 212.60(g), ICH Q7)

Warning Letter Trends: Data Integrity Related



- Based on warning letter issue date, through August 2018

Definitions

Data Integrity

- The extent to which all data are complete, consistent, accurate, trustworthy and reliable throughout the data lifecycle.

Data Lifecyle

- All phases in the life of the data, including generation, processing, reporting, archival, retrieval, and destruction.

ALCOA

- Data should be attributable, legible, contemporaneous, original, and accurate.

ALCOA +

- Plus complete, consistent, enduring, and available.

Definitions

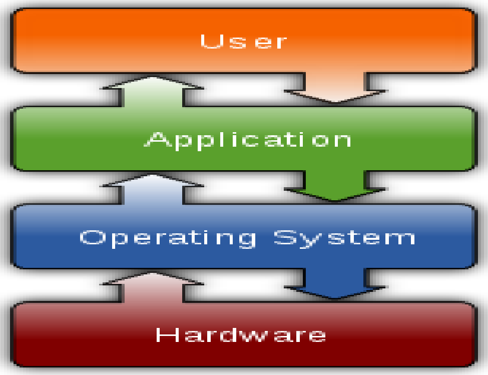
Metadata

- Data about data. Metadata are data that describe the attributes of other data, and provide context and meaning. Data that describes the structure, data elements, inter-relationships and other characteristics of data.

Data Governance

Data Governance

- The sum total of controls to ensure that data, irrespective of the format in which it is generated, are recorded, processed, and retained to ensure a complete, consistent, accurate, enduring and available record throughout the data lifecycle.



Data Integrity Policy

- The policy should demonstrate
  - Management understanding & commitment to effective data governance
  - Combination of appropriate culture and behaviors
  - Understanding of data criticality, risk and lifecycle
  - Communication at all levels in organization to report data integrity failures and opportunities for improvement – Train the Staff

- **Goal**
  - **Eliminate falsification, alteration and deletion of data**

(Source: Draft PIC/S Good Practices for Data Management & Integrity – Aug 2016)

Practical Application of Data Integrity Policy

- Designate a Data Integrity / Anti-Fraud Officer
- Conduct data integrity based audits outside of regular audit schedule
- Use CAPA system to document, investigate, correct and prevent data integrity issues

“Suspected or known falsification or alteration of records required under parts 210, 211 and 212 must be fully investigated under cGMP quality system to determine effect on patient safety, product quality, and data reliability. Report DI issues at DrugInfo@fda.hhs.gov”

(Source: Draft Guidance – Data Integrity and Compliance with CGMP – FDA April 2016)

Data Integrity SOPs

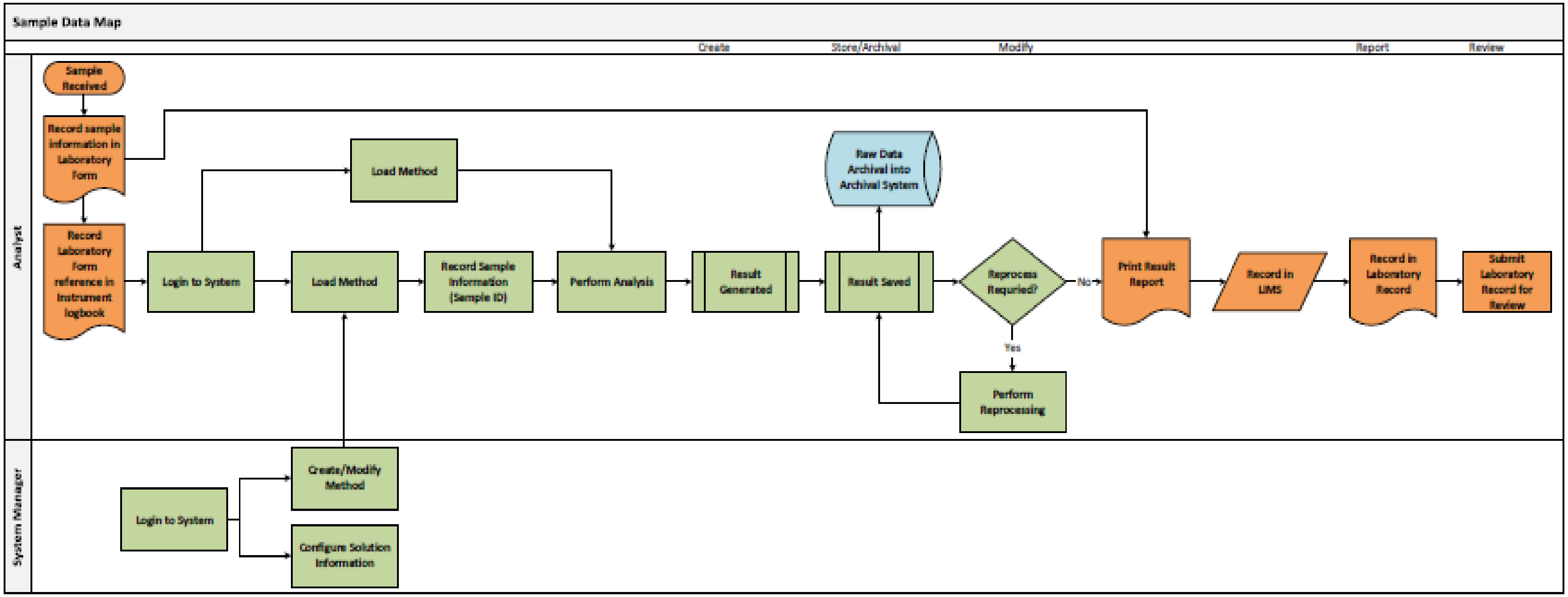
- IT policies (security, passwords, etc.)
- System use (data acquisition and processing)
- Data file naming conventions
- System administration (configuration, roles and privileges)
- Data review and approval
- Audit trail review
- Data back-up and archiving

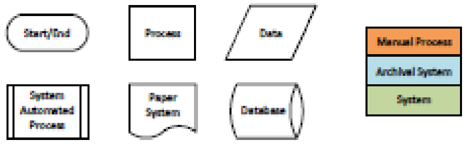
Creation of Data Flow Diagrams

- Validate your business workflows and data flows based on intended use

- Create system data maps
  - Describe how data are created, modified, reported and managed
  - Show relationship of system roles to functions within the data lifecycle
  - Describe audit trail components (lab forms, logbooks, software logs)
  - Describe controls – automated or procedural (software, hardware, personnel, documentation) – **Target full traceability of actions**

Creation of Data Flow Diagrams





Audit Trail Components

- Laboratory Form
- Logbook
- Software Audit Log
- Sample Analysis Details
- Standardization Information
- Standard Certification Information

Controls:

Access:

- Unique user ID and password required for Login to work station and application

Creation:

- Operators use naming conventions per Standard Operating Procedures.
- Only the System Manager can create new methods and configure solution information

Modification:

- The system audit log automatically records changes and user information when data is reprocessed.

Storage:

- Data is saved to system database automatically. User cannot delete or move the file.

Archival/Retrieval:

- System database file is stored to archival system on a daily basis. The archive undergoes backup on a nightly basis.

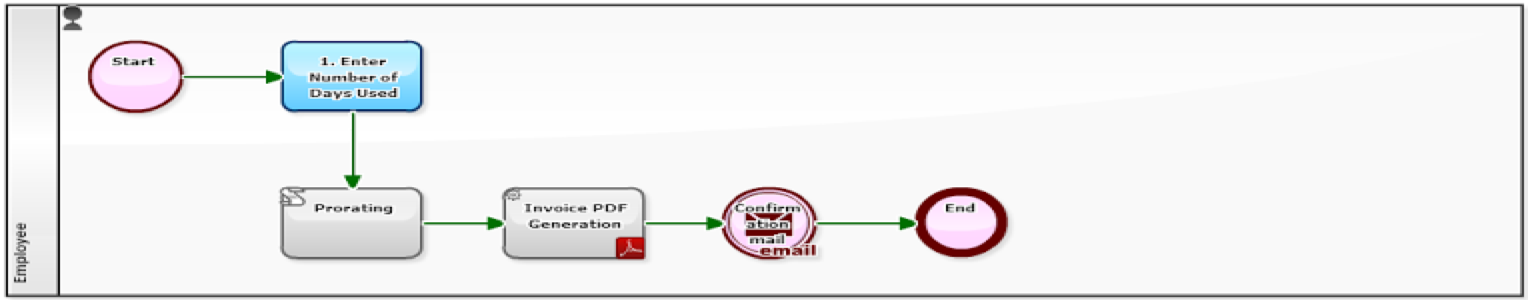
Auditors' Expectations

Be Prepared to discuss the following for each system:

- Electronic data
- Data storage, backup and archival
- The ability to modify or delete data
- User levels and associated privileges
- Audit trails and system logs
- Data and audit trail review

Electronic Data - Workflow

- How is data generated, i.e., what is the data flow for the system?
  - How is the data moved within the system?
  - Has the workflow been validated, including supporting processes and procedures?
  - Can file paths be changed to hide data?



Electronic Data – Backup/Archival

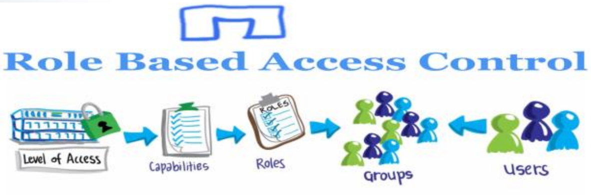
How is the data stored, backed-up and archived?

- Backup: True Copy of original data secured throughout retention period.
- How long is data stored and where?
- What is the data naming convention and is this defined in an SOP?
- Is the data backed-up? Is the data archived?
  - Where and How including frequency? Has this process been validated? Periodically re-tested?

Electronic Data – Data Alteration

- Can the data be modified or deleted – intentional or unintentional?
- Can the data be moved into a system trash bin or hidden in another system file?

User Levels & Privileges



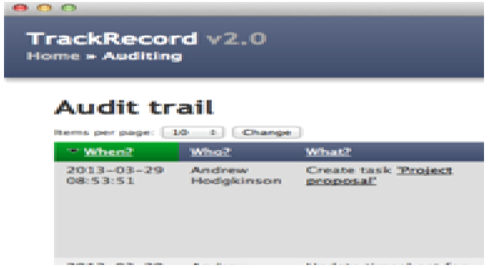
- How is access to the system authorized and controlled?
- Do you share system login credentials?
- What are the system user levels and privileges?
  - Typically – Operator, Manager, Administrator
  - Is there a good segregation of duties?
  - Are the user levels defined in an SOP?
  - Have system roles and rights been validated?
  - Can you provide a list of current and historic users and associated roles?

User Levels & Privileges

System Administration

- Is the administration role independent of the functional area?
- Can only the system admin configure critical settings within the system?
- Is the audit trial of the administrator being reviewed?

Audit Trails



TrackRecord v2.0

Home » Auditing

Audit trail

Items per page: 10 Change

When?	Who?	What?
2013-03-29 08:53:51	Andrew Hodgkinson	Create task 'Project proposal'

- Are system audit trails available?
  - Are they turned-on?
  - How are they different system logs?
  - Can they be disabled or deleted?
  - Can the system clock be modified to alter the audit trail?
  - Have audit trails been fully validated?
  - How are data modifications justified?
  - Has critical data been defined for the system?

Audit Trails - Review

- Do you have audit trail review procedures?
- Who conducts audit trail reviews? Quality Unit?
  - How are audit trail reviewers trained?
- What is the frequency of audit trail review?
  - How is the frequency justified?
  - FDA recommends:
    - Critical data be reviewed with each record and before final approval of the record
    - Review based on complexity of system and its intended use

(Source: Draft Guidance – Data Integrity and Compliance with CGMP – FDA April 2016)

Preparation of SMEs for DI Questions

- Know company policies and procedures regarding data integrity
- Have a system inventory list
  - include instrument/equipment type, software name/version, access control, data protection, audit trail, back-up system
- Know system instrument and equipment data flows/workflows
- Know user roles and privileges for each system
- Focus on System Operators/General Users
- Have a list of active users and associated roles ready for each system

Good Practices for SMEs

- Only answer the questions asked
- Know your equipment & software and how to trace the data record throughout the workflow
- Know where system audit trails are located
- Have full validation packages available for each equipment / instrument and related system – include supplemental testing of Part 11 / Annex 11 / Data Integrity controls

Preparation for Instrument/System Walk-Through

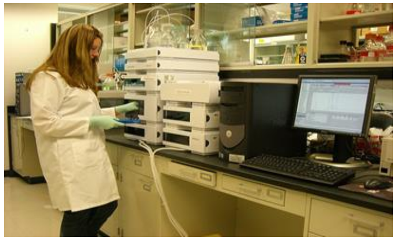
The Audit/Inspection

- Usually starts with a specific result or record
- Re-create sequence of events that occurred at the time the result or record was generated
- WHO, WHAT, WHEN, WHY
- Provide equipment / instrument and related software validation records

Preparation for Instrument/System Walk-Through

Auditor Checklist

- ✓ User profiles and passwords
- ✓ Roles and privileges
- ✓ System Administration
- ✓ Practical Tests – users attempt to:
  - ✓ Delete, over-write, move data
  - ✓ Open system trash folder
  - ✓ Change date / time functionality (lock the clock!)
  - ✓ Change system configuration or system role
  - ✓ Modify or delete the audit trail



Managing Findings, Prioritizing and Implementing CAPAs

- Perform internal data integrity based audits
- Must be fully investigated under cGMP quality system to determine effect on patient safety, product quality, and data reliability
- Prepare a CAPA plan
- Prioritize findings based on risk
- Commit to remediation – work with equipment & software vendors, show proof of intended software upgrades

Managing Findings, Prioritizing and Implementing CAPAs

- Demonstrate effective remediation by:
  - Hiring a third party auditor
  - Determining the scope of the problem
  - Implementing a corrective action and preventative action plan (globally) not in isolation
  - Removing at all levels individuals responsible for problems from cGMP positions

(Source: Draft Guidance – Data Integrity and Compliance with CGMP – FDA April 2016)

Overview of Common Findings / Issues

"The software that controls the [equipment / instrument] for NDA X were not validated. The firm did not validate the instruments data integrity acquisition system to ensure that analysts cannot re-write or delete analytical data during analysis. Data audit trails are not maintained and instrument audit logs are not saved."

Overview of Common Findings / Issues

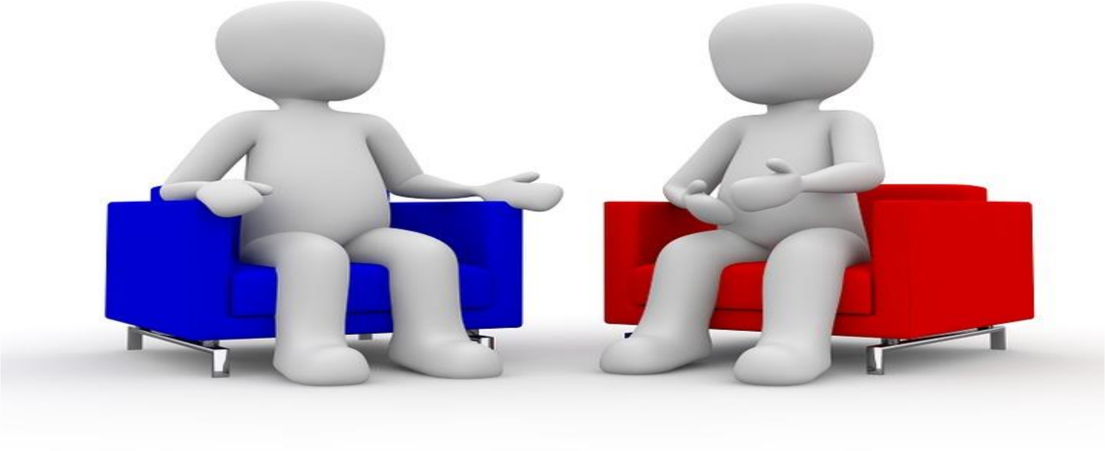
- Cited in numerous warning letters
  - No Audit trail or Audit trails were disabled
  - A shared username and password was used by many analysts
  - Users were able to manipulate, delete, or overwrite electronic raw data
  - Failure to maintain complete data

“Raises concerns about the validity and integrity of the data collected at your site.”

Q & A

Knowledge Exchange Session

- Share your audit / inspection experiences!



Thank You!

william.honeck@validation.org