PAI Inspections, Observations and Data Integrity

Krishna Ghosh, Ph.D.
Office of Pharmaceutical Quality
Office of Process and Facilities

Center for Drug Evaluation and Research

November, 2017

Agenda Topics

- Preapproval facility reviews and Inspections
- Risk frame work for PAI inspections
- PAI inspection objectives
- Inspection deficiencies and application withholds
- Inspections and Data integrity observations
- Data integrity policy Q and A's
- Data Integrity remediation and FDA expectation

Office of Pharmaceutical Quality

Office of Process and Facility

- This office evaluated the manufacturing process and facilities to ensure a robust process design, control strategy and Quality System can support commercial manufacturing of the product.

- OPF reviews the manufacturing and inspectional deficiencies
- Firms responses to FDA 483 and
- Final recommendation on facility for the application approval

Application- Manufacturing Process and Facility Reviews

- Before approval, FDA evaluates the sites that will manufacture the drug
- Determines if an inspection is required

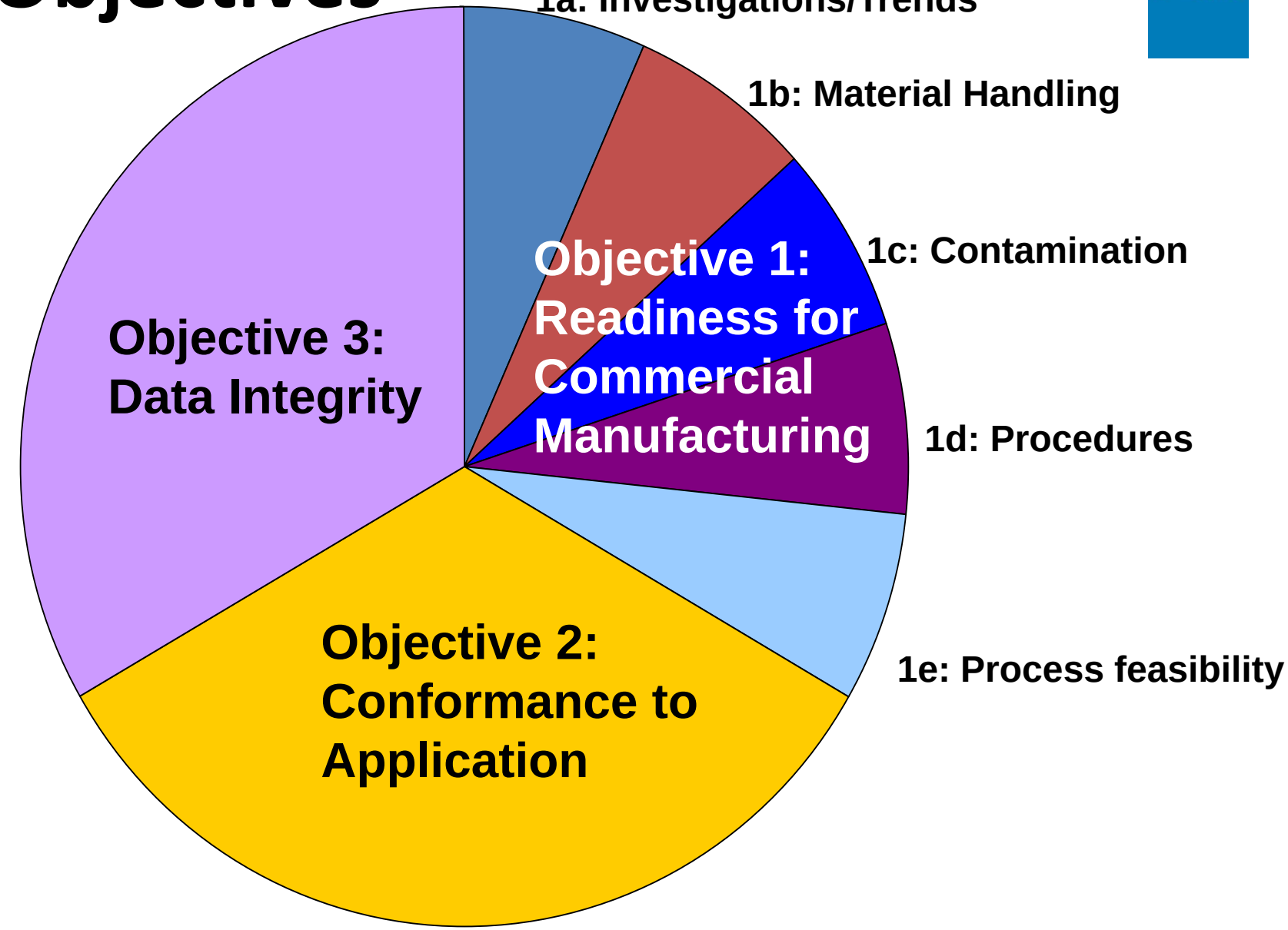
  The sites include:
  - Finished Dosage Form (FDF)
  - Active Pharmaceutical Ingredient (API)
  - Packaging
  - Testing Laboratories
  - Some complex intermediates

Risk Framework for PAI Inspections

FDA uses a risk-based facility assessment :

1. **Facility Risks**
   - Compliance history and current status
   - Recalls and field alerts
   - Observational Trends
2. **Process Risk** – Are there risks associated with the manufacturing process design and control strategy?
   - Type of dosage form
   - Inherent process complexities
   - Unique process characteristics
3. **Product specific Risk Factors-** Are there risks associated with the finished product characteristics?
   - Light and temp sensitive products
   - Combination Products
   - Radiopharmaceuticals/ PET Drugs
   - Low dose API products

PAI Objectives



Pre Approval Inspection
Some Common Reasons to Withhold

- Significant data integrity problems;
- Serious CGMP concerns with the manufacture of a bio-batch or demonstration batch;
- Significant differences between the process used for pivotal clinical batches and the NDA submission batch;
- Lack of adequate manufacturing process controls, written procedures, instructions in the master production record;
- Process validation batch failures;

Data that lacks integrity is….

Unreliable

- Omission of significant data from the submission that is determined to be material to the review process.
- Data that is not submitted, but should have been.

Inaccurate

- e.g., initial data failed specs, retest data passes specs, lab investigations are inadequate or non-existent, but retest data is submitted to the application.

Application Data & Application Integrity

All records are accurate representations of:

- Tests performed and test results
- Actual manufacturing & quality control
- Investigations and root cause analysis
- Unexplainable discrepancies between:
  - Data submitted to the FDA
  - Data found during inspection

Overall Facility Recommendations

If *any one* site is unacceptable:

- If any enforcement action is pending or has occurred; or
- If recent surveillance inspections show problems with currently marketed product; or
- If PAI specific issues are found
- Data Integrity issues have been identified which raises concerns on product quality and reliability of data in the application

Then the application is **NOT** approvable for the sites identified

Data integrity: Not a new concept

Principles from the paper-and-ink era still apply:

- 211.68 requires that backup data are exact and complete, and secure from alteration, inadvertent erasures, or loss.
- 212.110(b) requires that data be stored to prevent deterioration or loss.
- 211.100 and 211.160 require that certain activities be documented at the time of performance and that laboratory controls be scientifically sound.
- 211.180 requires true copies or other accurate reproductions of the original records; and
- 211.188, 211.194, and 212.60(g) require complete information, complete data derived from all tests, complete record of all data, and complete records of all tests performed.

API - ICH Q7

Computerized systems (5.4):

- Computerized systems should have sufficient controls to prevent unauthorized access or changes to data. There should be controls to prevent omissions in data (e.g., system turned off and data not captured). There should be a record of any data change made, the previous entry, who made the change, and when the change was made.
- If system breakdowns or failures would result in the permanent loss of records, a back-up system should be provided. A means of ensuring data protection should be established for all computerized systems.

Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients

Draft guidance

Data Integrity and Compliance With CGMP, draft guidance for industry (April 2016)

- Why? FDA has increasingly observed CGMP violations involving data integrity during Surveillance and PAI inspections.

- Ensuring data integrity is an important component of industry's responsibility to ensure the safety, efficacy, and quality of drugs, and of FDA's ability to protect public health.

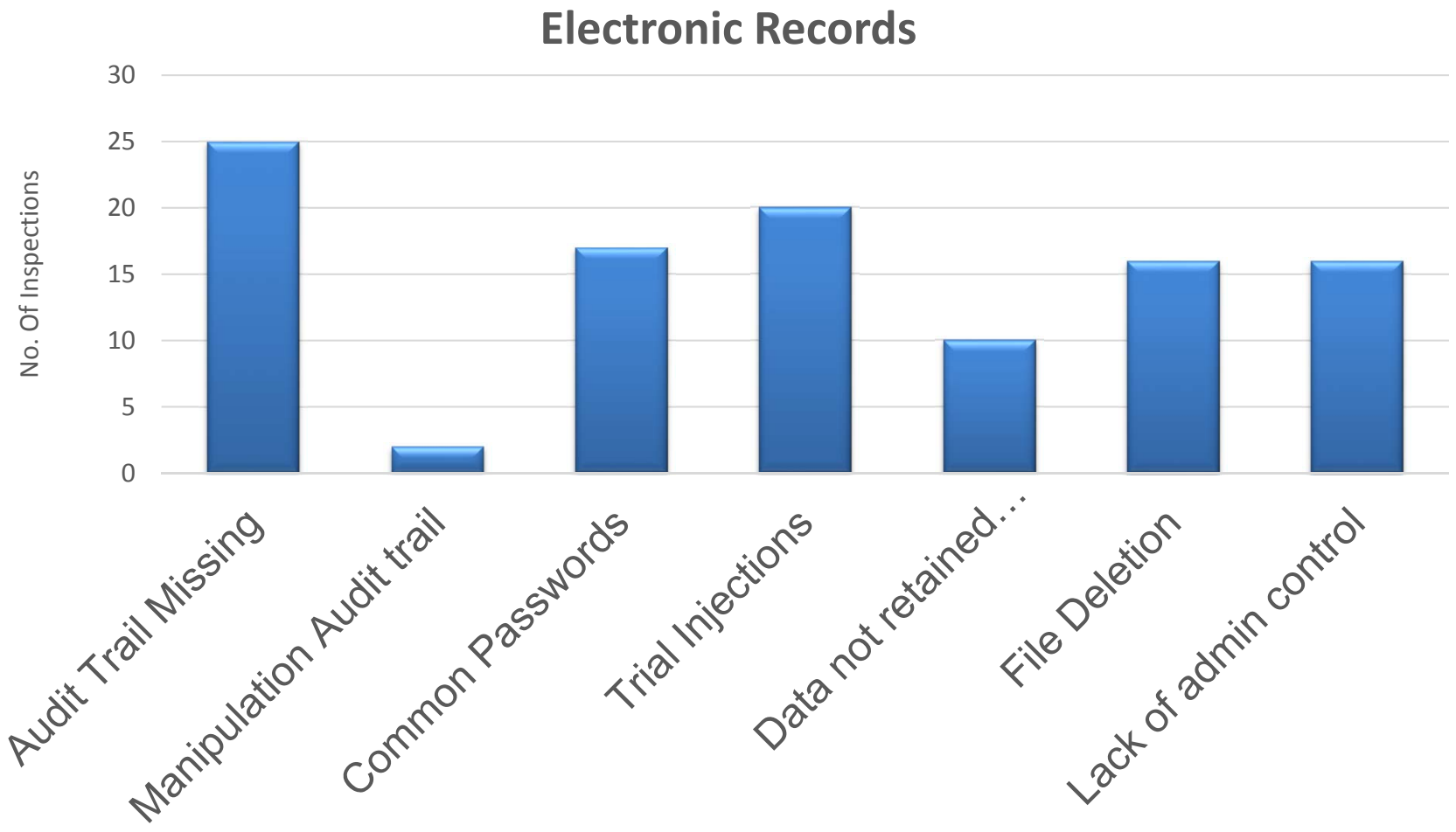
Available at www.fda.gov/downloads/drugs/guidancecompliancere gulatoryinformation/guidances/ucm495891.pdf

Data Integrity Trends

- 181 cases of OAI classification from all foreign inspections were identified and reviewed between 2010-2015.
- 141 cases were related to data integrity issues and rest were CGMP observations.
- Approximately 55% were paper records and 45% were electronic.

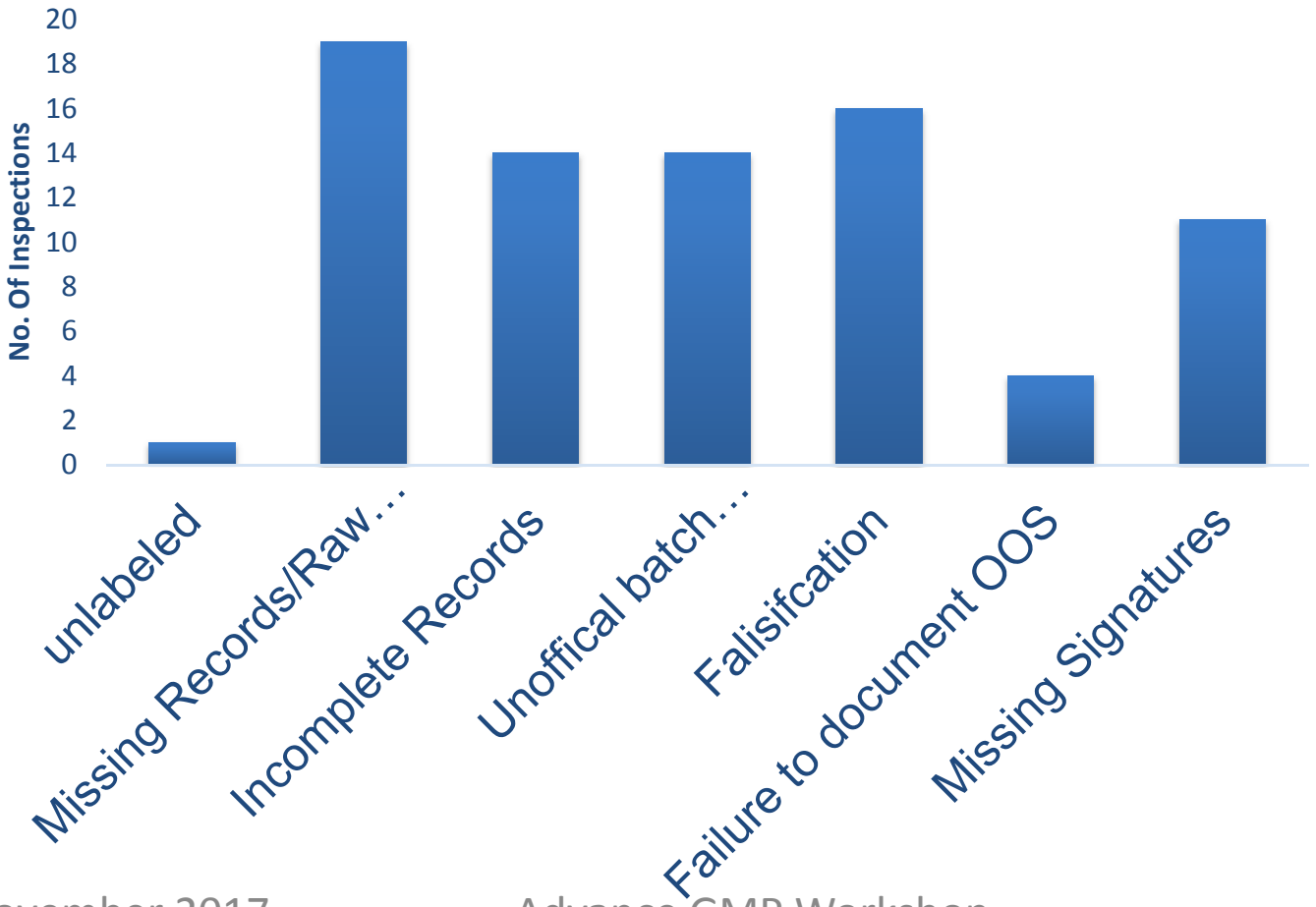
Data Integrity Observations

Distribution of Electronic Data Observations



Data Integrity Observations

Distribution of Paper document observations



Data Integrity Observations

Observations related to CGMP Systems

Data Integrity Concepts

- Metadata
- Audit Trail
- Static vs. Dynamic Records
- Backup Data
- System Validation

What is ‘metadata’?

- Contextual information required to understand data
- Structured information that describes, explains, or otherwise makes it easier to retrieve, use or manage data
- For example: date/time stamp, user ID, instrument ID, audit trails, etc.
- Relationships between data and their metadata should be preserved in a secure and traceable manner

What is an ‘audit trail’?

- Secure, computer-generated, time-stamped electronic record that allows for reconstruction of events relating to the creation, modification, or deletion of an electronic record
- Chronology: who, what, when, and sometimes why of a record
- CGMP-compliant record-keeping practices prevent data from being lost or obscured

Audit trails capture…

- Overwriting
- Aborting runs
- Testing into compliance
- Deleting
- Backdating
- Altering data
- *(not an all-inclusive list)*

Use of “static” and “dynamic” in relation to record format

- Static: fixed data document such as a paper record or an electronic image
- Dynamic: record format allows interaction between the user and the record content such as a chromatogram where the integration parameters can be modified

What are 'systems' in 'computer or related systems' in 211.68?

- Computer hardware, software, peripheral devices, networks, cloud infrastructure, operators, and associated documents (e.g., user manuals and standard operating procedures).

Case study: Audit trails off

- Raw data was being deleted or altered on IR spectrometer
- No access controls
- No **active** audit trails on IR
- File names altered to make it appear tests supported additional lots of API

Warning letter: *Lack of audit trails for lab instruments and turning off audit trails. (April 2015)*

Case study: Audit trail review

- Observed repeat GC injections in the audit trail in June 12, 2013.
- Audit trail showed the computer date/time settings were set back in July 2013 to June 12, 2013 (audit trails go in chronological order, but the dates didn't and showed multiple June 12ths).
- Results were reprocessed and printed to show that they had achieved passing results on June 12, 2013.
- Firm relied on this data to release the batch.
- Similar situation was observed for HPLC testing.

Warning letter: *Because your quality unit did not review the original electronic raw data, you were unable to detect rewritten, deleted, or overwritten files. (*January 2015)

Who should review audit trails?

- Audit trails are considered part of the associated records.
- Personnel responsible for record review under CGMP should review the audit trails that capture changes to critical data…as they review the rest of the record.

When is it permissible to exclude CGMP data from decision making?

- Data created as part of a CGMP record must be evaluated by the quality unit as part of release criteria and maintained for CGMP purposes.
- Electronic CGMP data should include relevant metadata.
- To exclude data from the release criteria decision-making process, there must be a valid, documented, scientific justification for its exclusion.

Does each workflow on our computer system need to be validated?

- Yes, a workflow, such as creation of an electronic MPCR, is an intended use of a computer system to be checked through validation.
- If you validate the computer system, but you do not validate it for its intended use, you cannot know if your workflow runs correctly.

How should access to CGMP computer systems be restricted? (continued)

- Recommend system administrator role, including any rights to alter files and settings, be assigned to personnel independent from those responsible for the record content.
- Recommend maintaining a list of authorized individuals and their access privileges for each CGMP computer system in use.
- Recommend restricting the ability to alter:
  - Specifications
  - Process parameters
  - Manufacturing or testing methods

Case study: Administrator privileges

Warning letter: *We observed systemic data manipulation across your facility, including actions taken by multiple analysts and on multiple pieces of testing equipment.*

Specifically, your Quality Control (QC) analysts used administrator privileges and passwords to manipulate your high performance liquid chromatography (HPLC) computer clock to alter the recorded chronology of laboratory testing events. (May 2016)

Why is FDA concerned with the use of shared login accounts for computer systems?

A firm must:

- Exercise appropriate controls to assure that only authorized personnel make changes to computerized records
- Ensure actions are attributable to a specific individual.

Case study: Shared logins

- No passwords were required to login.
- Anyone who accessed the system had full software administrator privileges.
- An analyst stated that **someone else had used their login** to delete and modify data.

Warning letter: *Provide specific details of the steps you have taken to prevent unauthorized access to your electronic data systems and to ensure that data systems retain complete, accurate, reliable, and traceable results of analyses performed. (November 2015)*

How should blank forms be controlled?

- Blank forms (e.g., worksheets, laboratory notebooks, and MPCRs) should be controlled by the quality unit or by another document control method.
- Numbered sets of blank forms may be issued and should be reconciled upon completion of the activity.
- Incomplete or erroneous forms should be kept as part of the permanent record along with written justification for their replacement.

What is wrong with using samples during 'system suitability' or test, prep, or equilibration runs?

- FDA prohibits sampling and testing with the goal of achieving a specific result or to overcome an unacceptable result.
- For example: using test, prep, or equilibration runs as a means of disguising testing into compliance.

What is wrong with using samples during 'system suitability' or test, prep, or equilibration runs?

- If a sample is used for system suitability:
  - It should be a properly characterized secondary standard.
  - Written procedures should be established and followed.
  - Sample should be from a different batch than the sample(s) being tested.
- All data should be included in records retained and subject to review unless there is documented scientific justification for its exclusion.

Is it acceptable to only save the final results from reprocessed laboratory chromatography?

- No.
- Analytical methods should be validated and be able to demonstrate repeatability
- Analytical processing methods should be standardized and repeatable
- If reprocessed, written procedures must be established and followed.
- FDA requires laboratory records include complete data derived from all tests.

How does FDA recommend data integrity problems identified during inspections be addressed?

- Demonstrate effective remediation by:
  - Hiring third party auditor based on scope
  - Determining scope of the problem
  - Implementing corrective action plan (globally)
  - Removing individuals responsible for problems from CGMP positions
- FDA may re-inspect

Responding to Data Integrity Failures

Data Integrity section in recent FDA Warning Letters with data integrity citations, requests firms respond with 3 key pieces:

- Comprehensive Evaluation (Scope)
- Risk Assessment (Scope)
- Remediation and Management Strategy (including corrective action plan)
- Risk to reliability of submitted application data that serves the basis of review and approval.

Comprehensive investigation

A comprehensive investigation should include:

- **Detailed investigation protocol and methodology**; summary of all laboratories, manufacturing operations, and systems to be covered; justification for anything to be excluded.
- **Interviews of current and former employees** to identify the nature, scope, and root cause of data inaccuracies. Should be conducted by a third party.
- **Assessment of the extent of data integrity deficiencies**. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion. Describe all operations with data integrity lapses.
- **Comprehensive retrospective evaluation** of the nature of the data integrity deficiencies. Qualified third party with expertise specific to firm's breaches should evaluate the lapses.

Risk assessment & management strategy

- A current **risk assessment** of the potential effects of data integrity failures on the quality of your drugs.
- Should include analyses of risks to patients due to release of drugs produced with data integrity lapses as well as risks posed by ongoing operations.

Management strategy

- A **detailed corrective action plan** that describes how you intend to ensure the reliability and completeness of all of the data you generate, including analytical data, manufacturing records, and all data submitted to FDA.
- A comprehensive description of the **root causes** of your data integrity lapses, including evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. **Indicate whether individuals responsible for data integrity lapses remain able to influence CGMP-related or drug application data at your firm.**
- **Interim measures** describing the actions you have taken or will take to protect patients and to ensure the quality of your drugs, such as notifying your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, drug application actions, and enhanced complaint monitoring.
- **Long-term measures** describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of your company's data.
- A status report for any of the above activities already underway or completed.

THANK YOU!

QUESTIONS?