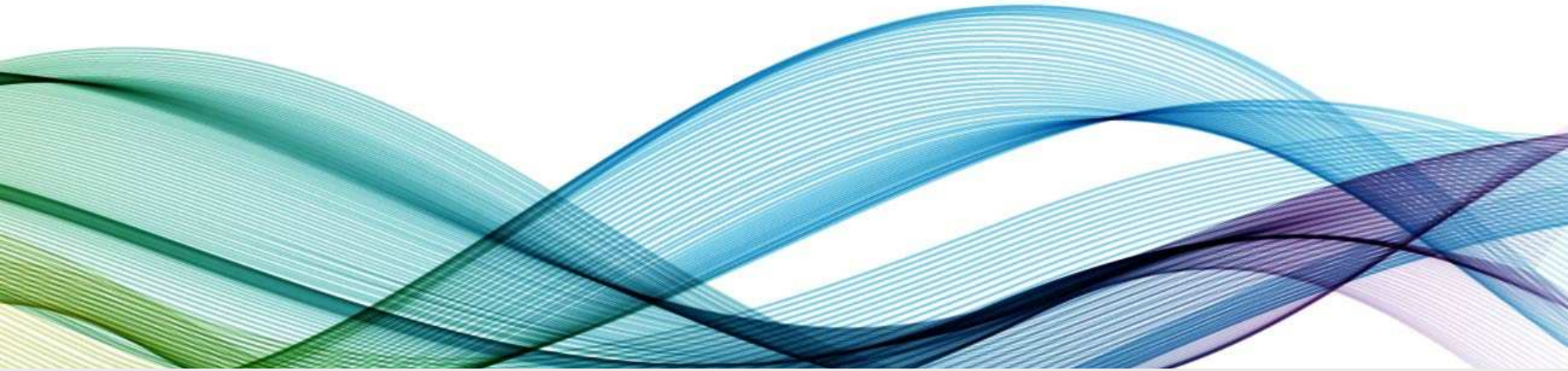
A Comprehensive Approach to Find and Remediate Data Integrity Problems

June 14, 2017



What is data integrity? Whom does it apply to?

Definitions matter

WHAT: Regulators perspective

"The degree to which a collection of data is complete, consistent and accurate."

UK Medicines and Healthcare Products Regulatory (MHRA)

"Data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)."

U.S. Food and Drug Administration (FDA), DRAFT Guidance for Industry: Data Integrity and Compliance With CGMP, April 2016.

WHO: The entire pharmaceutical supply chain

- Research
- Manufacturing
- Distribution
- Non-clinical / Clinical testing services

Why data integrity matters

Public health is at risk

- Unlike other industries, the difficulty in **detecting pharmaceutical quality issues**, which are often not visually detectable, **increases our dependency on product data**
- **False data** purporting that product meets specifications for the identity, quality, purity, or potency **undermines our reliance on product safety and effectiveness**
- This may cause:
  - Patient injury
  - Drug shortages
  - Damage to corporate reputation
  - Lost profits
  - Civil and / or criminal liability

It’s all about trust…

Once trust is lost with customers, patients and regulators, it can be difficult if not impossible to gain back

QuintilesIMS™

Why data integrity now?

Trust has always been important, so why the current focus on data integrity?

Globalization of pharmaceutical supply chain

- Speed of growth and competitive dynamics increase pressures on manufacturers
- Lab data is “ground zero” for data integrity – unreliable data = “guilty until proven innocent”

Diffusion of Responsibility

- More suppliers and partners contribute to the product and its support
- More mergers and acquisitions have led to disparate systems and less than full integration

Process complexity

- It is difficult to see end-to-end
- More automation and technology employed leading to more metrics and measurements

Cost pressures

- Industry contraction translates to making more with less
- Quality systems are strained

Today's agenda

Time	Topic
1:00-1:30 pm	Robust definition for data integrity
1:30-2:30 pm	Examining your organization: • How far back do we go? • Tools to consider
	How do we approach a remediation strategy? What risk-based strategies work best?
2:30-3:00 pm	Some examples of Data Integrity within current operations: • Manual Systems • Automated Systems • Lab Operations • IT Systems
3:00-3:15 pm	**Break**
3:15-4:15 pm	Case examples: Review of recent Form 483's and structuring the CAPA • Case Examples One: • Case Example Two:
4:15 pm-close	Round Table: Discussion Developing a DI strategy • Where do I start? • What do I consider?

Principles of data integrity

ALCOA

In order for data to have integrity it needs to follow the principles of data integrity, which means it is **ALCOA**:

Principle	Requirement
Attributable	Data includes information captured in the record uniquely identifying the originator of the data
Legible	Data is readable (not obscured), traceable to the source and permanent
Contemporaneous	Data is captured or recorded at the time it was generated or observed
Original	Data is the first or source capture of the data or a certified “True Copy” preserving the content and meaning of the original data
Accurate	Data is correct (free from error), truthful, valid and reliable

Principles of data integrity

ALCOA+

Once the integrity of data is established it needs to be maintained throughout its lifecycle. If at any point its data integrity is lost, it cannot be re-established!

Therefore, it is paramount that data integrity, once established, is managed by the following **ALCOA+** principles:

Principle	Requirement
Complete	All data and relevant metadata, including any repeat or reanalysis performed, must be maintained
Consistent	Data should be created and modified in a consistent, repeatable manner
Enduring	Data is recorded in a permanent, maintainable form throughout its retention period
Available	Data is accessible for review and audit or inspection over throughout its retention period

FDA Draft Guidance for Industry

Data Integrity and Compliance with CGMP, April 2016

Data integrity:

- Is analogous with possessing the attributes of ALCOA and is the original or a true copy

Explains the concepts of:

- Metadata
- Audit trail
- Static vs. dynamic records
- Backup
- Systems

Provides guidance on:

- When electronic data must be part of cGMP record
- When GMP data may be excluded from decision making
- Workflow validation
- Electronic signatures
- Training
- FDA access, and
- Issue remediation

Data integrity findings

By the numbers

5x increase in FDA cited data integrity issues since 2010

12 Warning Letters with DI findings in 2015, most DI findings of any year to date

97% of findings still arise from locations outside the U.S. (but that's changing)

Most Common FDA Finding:

Your firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 211.194 (a))

- "Trial" sample data was not kept as part of the data for the batch
- Sample weights, sample preparation and sample dilutions were not retained
- Deleted data detected in audit trails
- Overwriting data
- Discarded data recovered from trash
- Duplicate log books kept

QuintilesIMS™

Cost of inadequate data integrity

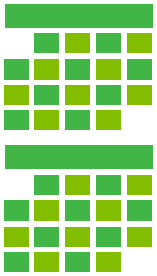
Financial impact is real

Fastest time to resolve 483 findings = 6 months

Average typical time to resolve 483 findings = 12 months

Can take up to 2 years to resolve 483 findings

Warning Letters are often longer to resolve



WL for cGMP and Testing Issues: **2 years to close at a cost of $64 million**

- Lost revenue and hard costs: facility projections reduced by $20 million; $35 million in remediation costs
- Opportunity cost on product with 20% ROCE, reduced profits by $9 million

QuintilesIMS™

Recent data integrity related FDA Warning Letter excerpts

Zhejiang Hisoar Pharmaceutical Co. Ltd. 8/11/16

Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established specifications and standards.

During the inspection, FDA investigators discovered a **lack of basic laboratory controls to prevent changes to your electronically-stored data and paper records**. When you encountered suspect and out-of-specification (OOS) results, you retested samples until you obtained desirable results. You did not investigate, review, or report original results. You relied on incomplete records to evaluate the quality of your drugs and to determine whether your drugs conformed to established specifications and standards.

Failure to prevent unauthorized access or changes to data, and to provide adequate controls to prevent manipulation and omission of data.

During the inspection, we observed that your laboratory systems **lacked access controls to prevent deletions or alterations to raw data**. For example, our investigator reviewed the electronic folder containing data files generated when your firm tested batches of API for residual solvents by gas chromatography (GC). The investigator compared the file names in the folder with the metadata generated by the Chemstation software you used to operate your GC system, and found that two chromatograms had been deleted from the system.

FDA Warning Letter, Jan 30,2015: Emphasis Added

Recent data integrity related FDA Warning Letter excerpts

Chongqing Lummy Pharmaceutical Co. Ltd. 6/21/16

Failure to prevent unauthorized access or changes to data and failure to provide adequate controls to prevent manipulation and omission of data.

During the inspection, FDA's investigator discovered a **lack of basic laboratory controls to prevent changes to and deletions from your firm's electronically-stored data**. Your firm relied on incomplete and falsified records to evaluate the quality of your drugs and to determine whether your drugs conformed with established specifications and standards.

Our investigator found that your firm failed to prevent data manipulation on multiple computerized analytical systems. Your firm re-tested samples without justification and deleted raw analytical data from computerized systems.

Failure to document manufacturing operations at the time they are performed.

During the inspection, our investigator reviewed 20 executed batch manufacturing records and found that most of them **contained similar or identical entries** that could not be adequately explained. For example, our investigator examined batch records for different batches of API manufactured between January and February 2015. All batch records indicated that certain process steps or measurements had transpired at exactly the same time for each different batch.

FDA Warning Letter, Jan 30,2015: Emphasis Added

Systems inventory and initial risk categorization

Business Units need to create and maintain a Systems Inventory of all systems generating data within their functional unit.

The systems in each Business Unit should be assessed for criticality by identifying the severity of harm (S) to product quality or to the patient, and probability of occurrence (P), i.e., S * P = **RISK**, using the table below.

The assessed system's risk category should be noted in the Systems Inventory, along with the date the system was put into service.

Risk Category	Risk Indicators
Low	No Impact, system generates data but it is not used for a product quality or patient safety
Medium	Some Impact, system generates data tangentially impacting a product quality or patient safety, e.g., FIO in-process measurements, non-critical utilities
High	Direct Impact, system generates data impacting a product quality or patient safety and may be directly related to a critical process parameter or an in-process control with a direct link to a Critical Quality Attribute (CQA) or safety data
Critical	Critical Impact, system generates data for a CQA or safety data

Risk category should be reassessed if the systems' scope changes.

Periodic data integrity gap assessment

Following the Initial Risk Categorization, the Business Unit and Data Integrity Steward needs to conduct and document a risk-based Periodic Data Integrity Gap Assessment to identify any potential data integrity gaps for each system in the System Inventory.

The frequency of this assessment is based upon the system's assessed Risk Category, cross-referenced with the table below.

The Gap Assessment should be conducted using the appropriate Gap Assessment Form (Paper or Electronic).

Risk Category	Risk Indicators
Low	Every 5 years
Medium	Every 3 years
High	Every 2 years
Critical	Annually

Other tools to address data integrity problems

Employ the right tools to ensure comprehensive awareness of DI issues

Governance

Leadership and accountability at all levels for data integrity is a critical success factor to addressing and maintaining a culture which supports data integrity

- Decide under which Office this issue will reside (CIO, CQO, etc.)
- Integrate DI into executive communications
- Gain support for DI remediation from impacts departments

Quality System

Employ current Quality System tools to address issues as they arise

- Audit programs
- CAPA and Deviation Management
- Change Control
- Training
- Controlled Document Management

Tools

Create and maintain tools to assess risk, identify gaps, and implement coordinated changes to impacted processes and systems

Break Out Session Part 1

Create the strategy and develop the approach

Strategy Components

- **Stakeholders**
  - e.g., patients, executive management, regulators
- **Communications**
  - e.g. sender, audience, training considerations, venues
- **Process approach**
  - e.g. top down, bottom up, risk-based, other

Approach Considerations

- Where do we begin?
- Which Quality Management System levers do we employ?
- Who is accountable to make this happen?
- What mechanism can we employ?
- Quality plans, vendor agreements, change control, CAPA, other
- What is our time frame?