FDLI

Enforcement, Litigation, and Compliance Conference

December 7-8, 2016
Washington, DC

Drug and Device: Warning Letters and Data Integrity

Frederick R. Ball, Partner, Duane Morris LLP

Raj D. Pai, Partner, Sidley Austin LLP

Robert A. Rhoades, Senior Vice President, QuintilesIMS

Interpretation of the FDA Data Integrity Draft Guidance & Preparing for Compliance

Frederick R. Ball, Duane Morris LLP

Robert A. Rhoades, QuintilesIMS

Raj Pai, Sidley and Austin LLP

December 7, 2016

Data Integrity

- cGMP sets the minimum requirements for data integrity

- Data integrity is critical to meeting cGMP

- FDA takes data integrity seriously

Consequences for Failure to Comply with Data Integrity Regulations

- Form 483s
- Warning Letters
- Import Alerts
- Recalls
- Complete Response Letters

FDA’s Draft Guidance

- Data Integrity and Compliance With cGMP, draft guidance for industry (April 2016)
- Q&A style guidance focused on frequently occurring problems with data integrity lapses and how they relate to cGMP in 21 C.F.R. § § 210, 211, and 212; clarifies the definition of key terms in FDA’s regulations.
- Is not a comprehensive list of data controls or a “how to” guidance.
- When final, it will represent FDA’s current thinking on data integrity and CGMP compliance.

What is Data Integrity?

- Data integrity – requirements for complete, consistent, and accurate data.

- Throughout cGMP

ALCOA
• **A**ttributable
• **L**egible
• **C**ontemporaneous
• **O**riginal or true copy
• **A**ccurate

Other Important Concepts

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

Paper and Electronic Records

- Same requirements for paper and electronic records:
  - § 211.68: back-up records complete, secure from alteration, erasure, or loss
  - § 212.110: data stored to prevent loss or deterioration
  - § § 211.110 and 211.160: activities be documented at the time of performance; scientifically sound laboratory controls
  - § 211.180: copies be true and accurate
  - § § 211.188, 211.194, and 212.60(g): complete information, complete data derived from all tests, complete record of all data, and complete records of all tests performed

Computer Systems

- cGMP-related computerized systems should be validated.
- Demonstrate the suitability of computer hardware and software to perform assigned tasks.
- Incidents related to computerized systems that could affect the quality the reliability of records or test results should be recorded and investigated.

Access to
cGMP Computer Systems

- Restrict the ability to alter specifications, process parameters, or manufacturing or testing methods by technical means where possible (for example, by limiting permissions to change settings or data).
- Assign the system administrator role, including any rights to alter files and settings, to personnel independent from those responsible for the record content.

When Does Electronic Data Become a cGMP Record?

- All Data generated to satisfy a cGMP requirement is a cGMP record.
- You must document, or save, data at the time of performance.
- If you record data on paper and then copy to the electronic record, you must retain the paper record.
- You may not do “test” runs that are not recorded.

Use of Samples During “System Suitability” or Test, Prep, or Equilibration Runs

- You may not conduct sampling and testing with the goal of achieving a specific result or to overcome an unacceptable result.

- You may not test into compliance.

How Often Should Audit Trails be Reviewed?

- You should review audit trails that capture changes to critical data with each record and before final approval of the record.

- You should regularly review audit trails related to: history of finished product test results, sample run sequences, sample identification, critical process parameters.

If You Find a Data Integrity Problem

- Handle through your internal compliance programs
- And should include:
  - Determining the Scope of the Issue
  - Discussions with Counsel
  - A plan for Remediation
- And likely will include:
  - Disclosure to Regulatory Authorities

Recent Warning Letter Citations Involving Data Integrity

- Failure to have sufficient controls to prevent unauthorized access and changes to data or omission of data
- Failure to investigate and resolve critical deviations
- Failure to record activities/data at time of performance
- Failure to ensure laboratory records include complete data from all tests
- Failure to establish/maintain procedures for quality audits
- Destruction of data
- Failure to identify data integrity issues

Required Responses to Warning Letters on Data Integrity Violations

- Comprehensive investigation and evaluation
- Risk assessment re reliability and completeness of quality information and effects on quality of drugs
- Management strategy
- Status report of above activities

Culture is the leading risk factor for compromising integrity and compliance*

Leadership may be lax in holding teams accountable to ethical & quality standards

- Lack of appropriate principles, systems, controls and oversight
- Fraud may be tolerated or encouraged

Financial success is often prioritized over product quality

- Unrealistic cost controls force inadequate investment in staffing, training and development, facilities, equipment, systems, controls, etc.

Autocratic leaders not interested in two-way communications or team engagement

- Staff work to “please the boss” vs. doing the right thing

**Source: David Gebler, Suffolk University*

Culture is the leading risk factor for compromising integrity and compliance*

Organizations may not be focused on innovation and continuous improvement

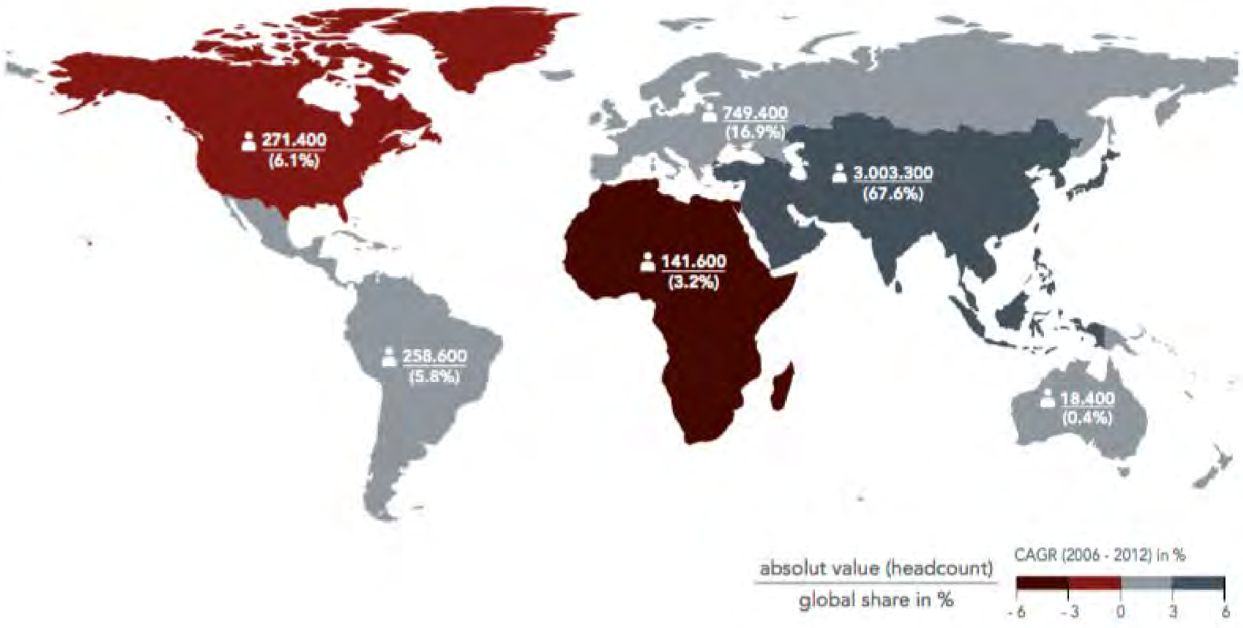
Large multinationals or departmental silos may limit communications & teamwork

Complacency, culture of fear, poor morale (e.g. post acquisition, layoffs)

Shallow focus on compliance vs. deeper understanding of product quality

Generics growth & globalization add layers of risk

*Global Pharmaceutical Employment**



- Production/employment is continuing to shift to emerging nations
- The patent cliff has resulted in volume flowing from few to many manufacturers (consistent to variable)
  - › Generics account for 88% of U.S. retail prescriptions (GPhA 2/16)
  - › ~ 80% of APIs and ~40% of finished drugs are imported
- Organizations may lack the financial strength or expertise to design & implement Quality Systems effectively
- Regulatory oversight while improving (e.g. FDASIA/GDUFA/OPQ) remains suboptimal

**Source: WiFOR Research Report, February 2015.*

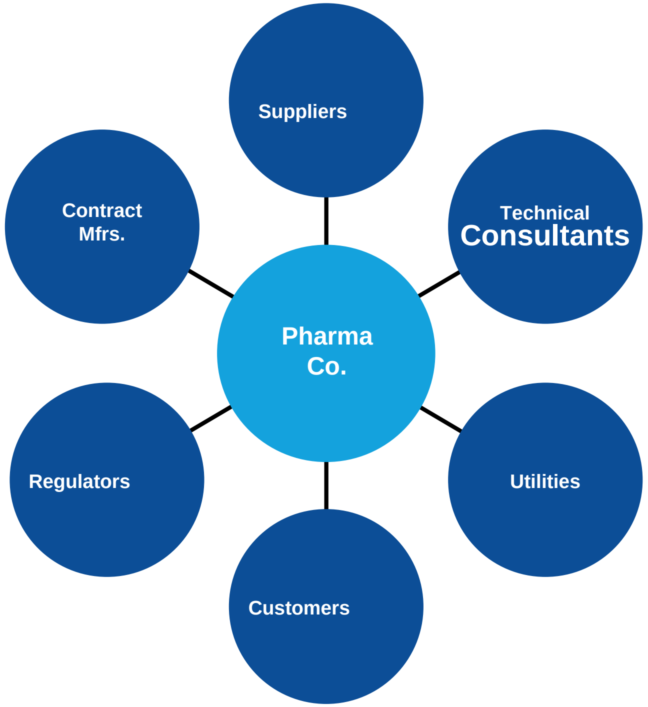
Other root causes of data integrity problems

Internal Quality System deficiencies and from suppliers & outsourcing partners

- *Weak ecosystem, systems, processes, equipment, and products that increase the risk of data integrity problems (amplified by the heightened focus on metrics by FDA/industry)*

Poor procedures, training gaps and/or lack of awareness of rules or requirements

- *Selective data collection/retention, backdating, retesting, failure to document/investigate problem findings, fraud*
- *Ignorance: not being aware of regulatory requirements and/or poor training*
- *Practices of inspecting quality into product (vs. quality at source)*
- *Shared passwords, lack of integrated systems, conflict of interest in various roles*



Human & system errors

- *Mistakes: e.g. transposing data such as 4.78 vs. 4.87*
- *Synchronization: errors that occur when data is transmitted from one computer to another*
- *Changes in technology, where one item is replaced when it becomes obsolete or no longer supported, making old records unreadable or inaccessible*

Other root causes of data integrity problems

Personal integrity problems

- *Willful falsification or fraud*
- *Fear of retaliation, job loss*
- *Poorly designed incentives*
- *Cognitive dissonance*
- *Normalcy bias*
- *Level of control and connectedness*
- *Perceived low risk of being caught*
- *Laziness, willingness to take short-cuts*
- *Selection of passing results and exclusion of those that are failing*
- *Unauthorized changes to data made post acquisition*
- *Backdating test results to meet the required commitments*
- *Creating acceptable test results without performing the test*
- *Using test results from previous batches to substitute testing for another batch*

Photo Source: Forbes.com

Five leading solutions for remediating & preventing data integrity problems

- Investigating and remediating data integrity issues through CAPA and other Quality Systems
- Creating a culture of quality
- Developing visible, engaged leadership that is committed to continuous improvement
- Recruitment and retention strategies that support sound GMP & GDP practices
- Practical balanced performance management

Being Proactive

- Impossible to predict which individual sites will have data integrity issues
- Not always at geographically remote sites or those with high production volume
- Not just in India or China – occurring in the U.S. and Europe
- Need to be proactive with all facilities – a data integrity issue at one facility often leads regulators to question whether a broader problem exists
- Evaluate issues that arise at one site to ensure they are not occurring at other sites

Being Proactive:
Taking Steps to Identify Issues

- Effective internal audit program puts the company in best position to self-identify data integrity issues
  - *Incorporate data integrity reviews into the audit program*
  - *Include data integrity component in the internal audit SOP*
  - *Train auditors to detect data integrity issues*
- Consider occasional third-party involvement
- Take seriously reports of data issues – initiate prompt investigations

Thank you!

FDLI