aam™
Association for Accessible Medicines

Biosimilars Council
A Division of the Association for Accessible Medicines

GRx+Biosims

# Data Integrity Overview

Derek Glover

September 5, 2018

Engineering the Future
of Generic + Biosimilar Medicines

# Legal Notice

The information displayed on these presentation slides is for the sole private use of the attendees of the seminar/training at which these slides were presented and reflects solely the opinion of the presenter. Mylan N.V. makes no representations or warranties of any kind, either express or implied, with respect to the contents and information presented. All original contents, as well as the compilation, collection, arrangement, and assembly of information provided on these presentation slides, including, but not limited to the analysis and examination of information herein, are the exclusive property of Mylan N.V. protected under copyright and other intellectual property laws. These presentation slides may not be displayed, distributed, reproduced, modified, transmitted, used or reused, without the express written permission of Mylan N.V.

# Laboratory Data Integrity

1. Laboratory Data Integrity Overview
2. Manual versus Electronic Systems
3. Computerized System Control
   - Vendor Management/Validation/FMEA
   - Understanding/Managing Computerized System Capabilities
   - Network versus Standalone systems
   - Legacy Systems and Interim Controls
   - Automation Considerations
4. Data Management/Verification Practices
5. Upstream versus Downstream Control Strategies

GRx+Biosims

Engineering the Future of Generic + Biosimilar Medicines

# Laboratory Data Integrity Overview

- Laboratory Data (Quality Control and AQL) represents a significant portion of critical quality attributes tested.
- ALCOA+ principles apply to all GMP data and firms need to fully understand the risk associated with their data given the broad variety of data acquisition systems being used.
- Training and validation alone cannot prevent a data integrity issue, additional controls are required to ensure the reliability of the data.
- Any gap in data integrity can result in a potential risk to the reliability of the application, the compliance of the facility, and the availability/safety of the product.

# Manual versus Electronic Systems

- Laboratory Data (Quality Control and AQL) can be acquired using both manual and electronic systems.
- Manual documentation processes must be carefully managed and second checks are often required to validate the accuracy and the contemporaneous nature of the data including, at times, the actual data acquisition (visual observation of a color titration).
- Electronic systems often provide more extensive features related to data security but are also more complex.  Without proper validation and control, the data may be just as vulnerable in these systems.

# Computerized System Control

**Vendor Management/Validation/FMEA**

- Compliance starts with careful procurement/partnership with the Vendor. Auditing of the vendor is critical to understand their design control and quality systems.
- GMP capability of the system needs to be tested rigorously. All data integrity principles need to be challenged.
- Firms need to establish robust User Requirements and overlay any vendor validation with specific internal CSV requirements/documentation.
- FMEA testing is often required to prove that an established control is effective (such as the user restriction for delete privileges).

# Computerized System Control

**Understanding/Managing Computerized System Capabilities**

- Avoiding tunnel vision. Systems often have additional functionalities that may not be directly related to the firm’s application but may have an impact on GMP compliance.
- Recycle bins, message centers, temp files, data purge features, etc. need to be fully understood and managed to mitigate risk to data reliability.
- Data processing and retention capabilities need to be enabled and validated.
- Audit trails need to be enabled, validated and reviewed.
- Data backup procedures need to be secure and routinely challenged.

# Computerized System Control

**Network versus Standalone Systems**

- Network connectivity can typically provide additional levels of security and can facilitate the data acquisition and backup process.  However, firms must be cautious to secure the network access given the connection versatility.
- Standalone systems can present challenges and risk related to user access, security, data retention, transfer, processing, etc.
- Hybrid systems that have partial computerized system control but utilize print features and/or manual data recording present a unique challenge.

# Computerized System Control

**Legacy Systems and Interim Control Measures**

- Older systems have a variety of challenges and need to be evaluated to determine any risk impacting the data.
- Interim control strategies need to be implemented to mitigate any risk identified.

**Automation initiatives** can create additional risk without careful planning.

- Assessment of PLC controllers for production equipment.
- Electronic Laboratory Notebooks.

Opportunity exists for alignment among industry partners, vendors and regulators to develop full understanding of the acceptable path forward with respect to computerized systems.

# Data Management Practices

- Control strategies are requisite to all lab data systems.
- Understanding how the data is used will inform the appropriate frequency of reviews, trending and inspection.
- Mapping the data is critical to understanding points of vulnerability.  (such as data exports, reformatting, etc)
- Signals such as system aborts, duplicate tests, data alteration, equipment malfunctions, deletion of anything, checksum failures, file corruptions, etc. should be investigated to a level commensurate with the risk.
- Manual documentation analogies should also be investigated appropriately.

# Upstream versus Downstream Control Strategies

Firms have historically relied on verification and review to detect any issues potentially impacting data.

- These solutions can be very labor intensive and may not serve to prevent issues from occurring.

Upstream data controls can serve to improve right first time and enhance detectability by minimizing the frequency of such issues.

  - Complete data calculations and entries prior to analysis.
  - Disallow single injections and institute strict oversight governing any changes/alterations to data/metadata.
  - Standardize naming conventions for data files.

GRx+Biosims
Engineering the Future of Generic + Biosimilar Medicines

# THANK YOU

**R. Derek Glover, Head of Global Quality Systems/Compliance**

Contact via LinkedIn

GRx+Biosims

Engineering the Future of Generic + Biosimilar Medicines