Data Integrity Policy

1 Purpose and scope

This policy sets out the principles for ensuring data integrity at FyoniBio GmbH. It applies to all data generated, recorded, processed and stored within the company, both in paper-based and electronic form. Adherence to the ALCOA^{++} principles is required.

All employees and contractors involved in drug development / clinical trial activities are required to recognize, comprehend and be compliant with this policy. Partners and vendors must be assessed to ensure their processes and systems meet this requirement.

Senior management will ensure that data integrity risk is assessed, mitigated and communicated in accordance with the principles of quality risk management. They are responsible for promoting a culture of data integrity and for ensuring that sufficient resources are available to meet the requirements.

2 Principles of data integrity

A risk-based approach in accordance with ICH Q9 (Quality Risk Management) is applied to ensure the appropriateness of the control measures. This involves assessing the data risk and data criticality for each phase of the data lifecycle. The measures to ensure data integrity are scaled according to the risk assessment to ensure efficient and effective control.

Computerized systems should be designed in a way that ensures compliance with the principles of data integrity. The system design should make provisions such that original data cannot be deleted and for the retention of audit trails reflecting changes made to original data.

Contracted service provider should apply equivalent levels of control to those applied by FyoniBio. FyoniBio will assess service provider's competency and compliance in this regard – e.g., by conduct of a qualification audit - prior to the conclusion of a contract.

2.1 Data Risk Assessment

Data risk assessment should consider the vulnerability of data to involuntary or deliberate amendment, deletion or recreation. Control measures which prevent unauthorized activity and increase visibility / detectability can be used as risk mitigating actions.

2.2 Assessment of data criticality

Points to consider regarding data criticality include:

- What decision does the data influence?
- What is the impact of the data to product quality or patient safety?

2.3 Data Life Cycle Management

Data integrity can be affected at any stage in the lifecycle. It is therefore important to understand the lifecycle elements for each type of data or record, and ensure controls which are proportionate to data

criticality and risk at all stages.

The 'Data lifecycle' refers to the:

- Generation and recording of data
- Processing into usable information
- Checking the completeness and accuracy of reported data and processed information
- Data (or results) are used to make a decision
- Retaining and retrieval of data which protects it from loss or unauthorized amendment
- Retiring or disposal of data in a controlled manner at the end of its life

Data should be reviewed at any life cycle stage of data. Data risk should be considered at each stage of the data lifecycle review.

2.4 Retiring or disposal of data

The following aspects should be considered when determining risk and control measures:

- The data retention period
- How data disposal is authorized

3 Training & awareness

All employees must complete data integrity training. Regular refresher training ensures that all parties are aware of new requirements and risks.

4 Responsibilities

FyoniBio employees are encouraged to report violations or concerns related to this policy. We ensure that reporting parties are protected from retaliation and offer anonymous and confidential reporting channels. All reported violations will be investigated and, where necessary, appropriate action will be taken to uphold our standards.

This policy will be regularly reviewed to ensure continued compliance with industry & regulatory requirements and best practice.