

1 Data Integrity Policy

Data integrity enables good decision-making by drug developers and regulatory authorities.

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 (see SOP-QM-004 Quality Audits).

Senior management will ensure that data integrity risk is assessed, mitigated and communicated in accordance with the principles of quality risk management.

A quality-risk management (ICH Q9) approach to data integrity can be achieved by considering data risk and data criticality at each stage in the data lifecycle. The effort applied to control measures should be commensurate with this data risk and criticality assessment.

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.

Risk based review of electronic data is acceptable.

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.

1.1 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.

1.2 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?

1.3 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.

1.4 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