Northern Ireland Blood Transfusion Service	POLICY DOCUMENT

Document Details

Document Number: POL:15:QP:014:01:NIBT **No. of Appendices:**

Supersedes Number: N/A

Document Title: DATA INTEGRITY POLICY

ISSUE DATE: **EFFECTIVE DATE:**

Document Authorisation

Written By :

Signature:_____ **Date :** _____

Authorised By :

Signature _____ **Date :**_____

Authorised By :

Signature: _____ **Date :**_____

CROSS REFERENCES

This Policy refers to the following documents:

Doc Type	Doc. No.	Title
POL	IP:006	GxP Computer Systems Compliance Policy
POL	IP:003	User Account and Password Management policy
POL	IGP:002	Records Management Policy
POL	IP:005	NIBTS Computer Security Policy
POL	IGP:003	NIBTS Information Governance Policy
SOP	QA:070	Procedure for reporting and management of quality

Key Change from Previous Revision:

New Policy

1. STATEMENT

Data integrity is a fundamental part of the Quality Management System to ensure product quality. Data integrity requirements apply equally to both paper records and electronic data throughout the product life cycle.

The aims of the Data Integrity Policy are:

- To provide guidance on data integrity principles and the implementation of these principles within NIBTS.
- To ensure that data integrity requirements are met appropriately, in line with current legislation and best practice guidelines.
- To set out the requirements NIBTS is expected to meet to ensure compliance with the GMP Standards published in Eudralex Good Manufacturing Practice regulations volume 4.

2. OVERVIEW

2.1 Data integrity is "the extent to which all data are complete, consistent and accurate throughout the data life cycle" (MHRA GMP Data Integrity Definitions & Guidance for Industry March 2015).

Data integrity requirements apply irrespective of the means by which data has been generated, or the format on which data is stored. Data may be generated by a paper based record of a manual observation, or a variety of simple machines, through to complex highly configurable computerised systems.

The risk to data integrity can vary depending on the degree to which the data or system generating the data can be configured and potentially manipulated. The complexity of computerised systems and the ongoing risk to data integrity should be assessed and reviewed periodically, in order to establish data criticality and

evaluate inherent risk to data integrity. The effort and resource applied to data integrity controls should be commensurate to both, data criticality and the level of risk.

Systems used by NIBTS should be designed in a way which encourages compliance with the principles of data integrity.

The purpose of this policy is to set out the requirements NIBTS is expected to meet to ensure compliance with the GMP Standards published in Eudralex volume 4.

3. RESPONSIBILITY

3.1 The NIBTS Senior Management Team (SMT) are responsible for ensuring compliance to the relevant regulations and monitoring the effectiveness of the processes put in place by their departments to protect data integrity.

3.2 Department Managers are responsible for implementing the guidelines included in this policy and ensuring any anomalies identified are reported via the incident reporting system.

3.3 Staff are responsible for ensuring they are:

- Fully committed to generate reliable data that is accurate, complete and timely.
- Accountable for the integrity of the data; including generation, recording, reporting and retention.
- To report situations of improper influence or of data misrepresentation to their Department Manager.

4. POLICY

4.1 Data integrity is a fundamental part of the Quality Management System to ensure product quality. Data integrity requirements apply equally to manual (paper) records and electronic data throughout all aspects of the data life cycle. For further information refer to NIBTS Information Governance Policy (IGP:003) and Records Management Policy (IGP:002)

- Raw data capture/initial generation.
- Manufacture (Process specifications, parameters and documentation).
- Processing (transformation/migration).
- Use (Product traceability and Pharmacovigilance).
- Retention.
- Archiving.
- Retrieval.
- Destruction.

The effort and resource assigned to data integrity controls should be commensurate with, the data criticality and the inherent risk to data integrity. The risk to data integrity may vary depending on the degree to which data or systems generating the data can be configured.

The criticality of data should be considered in terms of potential impact on product quality attributes. The assessment of both risk and criticality should be periodically reviewed and documented in order to ensure that data integrity arrangements in place provide an acceptable state of control.

Systems and procedures used by NIBTS should be designed to encourage compliance with the following principles of data integrity throughout the data life cycle.

	Paper / Electronic System considerations:
Attributable	Who acquired the data or performed an action and when
Legible/Permanent	Can you read (and understand) the data recorded, especially the audit trail entries?
Contemporaneous	Are data and activities recorded timely? Is there an electronic system clock synchronisation?
Original	Written printout or a certified copy thereof or documented backup of whole record. Does the metadata permit reconstruction?
Accurate	No errors or editing without documented amendments? How was the data captured?
Complete	All data present – none omitted or destroyed
Consistent	All elements of the record sequence of events follow on and are date or time stamped in the expected sequence.
Enduring	Recorded on controlled paper or electronic media
Available	Can the record be accessed for review, audit or inspection over the lifetime of the record?

Data Ownership
While NIBTS (SMT) has overall responsibility for ensuring compliance, departmental managers are nominated as “data owners” and are responsible for the integrity of data generated and managed within their department. These responsibilities are to ensure that data are acquired, secured, transformed and reported in accordance with defined procedures and that deviations will be documented and investigated.

Primary record
In cases where data are collected and retained concurrently by more than one method, the record which has primacy should provide the greatest accuracy, completeness, content and meaning.

Working Culture and Data Integrity Issues
The agency, under the guidance of the SMT, is committed to fostering a culture of responsible openness and constructive criticism to enable staff to raise and report data integrity issues.

Data Review and System Monitoring
A review of Paper and Electronic source data should be periodically reviewed on a risk based approach during self-inspection. Review may be non-contemporaneous data checking, unless verifying an observed value.

Furthermore, the compliance of systems (including legacy systems) with data integrity requirements should be reviewed periodically by the data owner, as required.

Data Integrity in relation to Computerised Systems
If the computerised system is configured for GxP compliance, then the audit trail and metadata must be backed up. A specification of which database / files are backed up should be defined and reviewed periodically. A copy of current (editable) data, metadata and system configuration settings (variable settings which relate to an analytical run) should be maintained for the purpose of disaster recovery. Backup and recovery processes must be validated. For further information refer also to, GxP Computer Systems Compliance Policy (IP:006).

Audit trails for computerised systems are available to system administrators of the computerised system. These audit trails should be validated, and proven that key information is recorded and the information recorded cannot be manipulated in any way.

All individuals should have a unique login to access the system. All user accounts are created following approval from a Departmental Manager / Deputy. A record of both current and historical user accounts should be maintained. All changes to user accounts should be documented.

The computerised system should use adequate password controls in line with the NIBTS User Account and Password Management policy (IP:003). PC's and electronic systems, should also be used in accordance with NIBTS Computer Security Policy (IP:005).

There should be a clear hierarchy of access levels for the system. These should be defined, validated and reviewed to ensure that the staff member only has appropriate access specific to their role. These should be periodically reviewed.

System Administrators have an independent role, and where this is not possible, they should have dual accounts to differentiate what is performed as a system administrator and what is performed as a standard user. All requests to delete data/configuration changes should be carried out using the appropriate documented procedure and be controlled via the NIBTS change management system as appropriate.

Data Integrity in relation to paper / hybrid systems
Computerised systems may support only a single user login or limited numbers of user logins, or have limited audit trail functionality. Where alternative computerised systems have the ability to meet user access control and audit trail requirements, facilities should upgrade to an appropriate system by the end of 2017. Where no suitable alternative computerised system is available, a paper based method of providing traceability will be permitted. The lack of suitability of alternative systems should be justified based on a review of system design, and documented.

Data retention
Data and document retention arrangements should ensure the protection of records from deliberate or inadvertent alteration or loss. Secure controls must be in place to ensure the data integrity of the record throughout the retention period, and validated where appropriate. Archive records should be locked such that they cannot be altered or deleted without detection and audit trail. The archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period.

The long term permanent retention of electronic data may require specialist intervention and should be undertaken in consultation with the IM&T and RA&C departments, and the system manufacturer. The long term archive of electronic data should be applied on a system by system basis with priority given to those systems approaching redundancy.

Incident reporting
Any data integrity incidents should be reported as a Quality Incident and the management of it should be managed as described in SOP:QA:070.

5. EQUALITY SCREENING OUTCOME

5.1 This policy has been drawn up and reviewed in light of the statutory obligations contained within Section 75 of the Northern Ireland Act (1998). In line with this statutory duty of equality this policy has been screened against particular criteria. If at any stage of the life of the policy there are any issues within the policy which are perceived by any party as creating adverse impacts on any of the groups under Section 75 that party should bring these to the attention of the Head of HR & Corporate Services.

The Northern Ireland Blood Transfusion Service is committed to the promotion of equality of opportunity for staff, donors and service users. We strive to ensure that everyone is treated fairly and that their rights are respected at all times. We believe that it is important that our policy is understood by all those whose literacy is limited, those who do not speak English as a first language or those who face communication barriers because of a disability. On request it may be possible to make this policy available in alternative formats such as large print, Braille, disk, audio file, audio cassette, Easy Read or in minority languages to meet the needs of those not fluent in English.

6. TRAINING REQUIREMENTS

6.1 NIBTS SMT is responsible for the implementation of systems and procedures to minimise the potential risk to data integrity This must include, as a component of on-going GMP training, a staff training programme that emphasises the criticality of the data integrity principles and the creation of an open reporting culture for errors and omissions.