Data Protection Policy

Author(s)	T. Bandason and T. Nyengerai
Approved By	
Approval Date	
Review Date	

THRU-ZIM DATA PROTECTION POLICY

This Data Protection Policy defines the principles, responsibilities, and conditions under which the Health Research Unit Zimbabwe (THRUZIM) of the Biomedical Research and Training Institute (BRTI) manages personal and research data in accordance with the Cyber and Data Protection Act [Chapter 12:07] (2021). It outlines THRUZIM's commitment to lawful, fair, and transparent data processing (CDPA Section 8), purpose limitation (Section 9), data minimisation and accuracy (Section 7), and implementation of appropriate security safeguards (Section 18). All inquiries regarding the interpretation or implementation of this policy should be directed to the THRUZIM Data Management Director (DMD) and Data Protection Officer (DPO).

1. INTRODUCTION

THRUZIM, operating under the Biomedical Research and Training Institute (BRTI), is committed to protecting the personal data of all individuals involved in its research activities. This Data Protection Policy outlines the principles and procedures by which THRU-ZIM ensures compliance with the Cyber and Data Protection Act [Chapter 12:07] (2021) of Zimbabwe (CDPA), the General Data Protection Regulation (GDPR), and other applicable international and institutional data protection frameworks.

This policy applies to all BRTI-THRUZIM staff, students, researchers, and collaborators (hereafter referred to as "Researchers") involved in the collection, processing, storage, sharing, and destruction of personal data within the scope of research activities. It establishes a foundation for data governance that upholds ethical conduct, enhances institutional accountability, and protects participant privacy across the research lifecycle.

2. PURPOSE

The purpose of this policy is to:

- Ensure lawful, fair, and transparent processing of personal data in line with applicable legal and ethical standards;
- Protect the rights and freedoms of data subjects (research participants), particularly in research involving sensitive or vulnerable populations;
- Define roles and responsibilities of researchers, data controllers, and data processors throughout the data lifecycle;

- Promote ethical, secure, and high-quality data handling practices consistent with international best practices;
- Support BRTI-THRUZIM's strategic vision to foster collaboration and responsible data sharing in global health research
- Ensure all research teams implement appropriate safeguards for personal and sensitive data, including consent, anonymisation, encryption, and secure retention.

3. SCOPE

This policy applies to all personal data collected, processed, or stored by BRTI-THRUZIM section researchers in the context of research projects, whether the data is held digitally or in paper format, and regardless of where it is stored, accessed, or transferred. The policy covers all research activities conducted under THRUZIM, including observational studies, clinical trials, implementation research, secondary data analysis, and programmatic evaluations.

It includes:

- Identifiable and de-identified participant data;
- Audio, visual, biometric, and geolocation data;
- Collaborator and staff data processed as part of research administration;
- Any third-party data provided under formal data-sharing agreements.

4. DEFINITIONS

- **Personal Data**: Any information relating to an identified or identifiable natural person, including names, contact details, ID numbers, photographs, and audio/video recordings.
- **Sensitive Data**: A subset of personal data including health information, sexual orientation, genetic/biometric data, ethnic origin, religious beliefs, and information concerning vulnerable populations (e.g., children, pregnant adolescents).
- **Processing**: Any operation performed on personal data, whether automated or manual, including collection, storage, use, transmission, disclosure, analysis, and deletion.
- **Data Subject**: An individual whose personal data is being processed.
- **Data Controller**: The natural or legal person or institution that determines the purpose and means of processing personal data (e.g., BRTI).
- **Data Processor**: An entity or person who processes data on behalf of the controller under a contractual or collaborative agreement.

5. DATA PROTECTION PRINCIPLES

BRTI-THRUZIM ensures compliance with the following key principles, aligned with the CDPA.

5.1 Lawfulness, Fairness, and Transparency

Processing is conducted on lawful grounds such as consent or public interest in research. Participants must be informed, in plain language, about how their data will be used, stored, and protected.

5.2 Purpose Limitation

Personal data must be collected for clear, specific, and legitimate research objectives. Any secondary use of the data must be compatible with the original purpose or ethically approved.

5.3 Data Minimisation

Only the data necessary to achieve the scientific objectives of the study will be collected. Researchers must avoid excessive or irrelevant data collection.

5.4 Accuracy

Data must be kept accurate and up to date. Mechanisms must be in place to correct or update inaccurate information, particularly in longitudinal studies.

5.5 Data Storage Limitation and Sharing

Data will be retained only for the duration necessary for research and regulatory reporting. Longer retention must be justified and documented.

Arrangement should be made for secure data storage throughout the study period in compliance with regulatory and contractual obligations. Researchers are responsible for ensuring that research data necessary to verify and reproduce the research findings are retained for a specified period and a minimum retention period of 10 years or longer may be specified.

Research data that substantiates research findings must be stored in centralised and recognised repositories or systems made available at the earliest possible time in compliance with ethical, legal or contractual requirements set up at the beginning of the research study. Research data not shared through data repositories must be shared using the available BRTI-THRUZIM data sharing channels which use established data sharing agreements. Appropriate security measures to unauthorised access, disclosure, alteration, or destruction should be set up and access to personal, sensitive, or confidential data restricted.

5.6 Integrity and Confidentiality

Security safeguards include physical access controls, secure servers, password protection, encryption, anonymisation, and staff training in data protection.

5.7 Accountability

Researchers and BRTI-THRUZIM must be able to demonstrate compliance with these principles through audits, documentation, ethics approvals, and data management plans.

6. RIGHTS OF DATA SUBJECTS

BRTI-THRUZIM recognises and protects the rights of data subjects as required under the Cyber and Data Protection Act (CDPA) [Chapter 12:07], Section 14, including:

- The right to receive clear and accessible information about data processing (transparency);
- The right to access their personal data and obtain a copy upon request;
- The right to correct or delete personal data if inaccurate, outdated, or unlawfully processed;
- The right to object to data processing, particularly for purposes unrelated to the original consent;
- The right to withdraw consent at any stage without affecting participation or service provision.

7. DATA OWNERSHIP

In addition to individual rights, BRTI-THRUZIM establishes institutional data rights and ownership obligations:

- Data rights and responsibilities must be agreed upon at the earliest stage when collaborating with external institutions;
- Exclusive ownership of research data must not be transferred to collaborating institutions unless required by a legally binding contract, duly approved by the Research DMD, DPO and BRTI-THRUZIM Directors;
- Where no explicit agreements exist, BRTI-THRUZIM retains primary ownership of all research data;
- Collaborating institutions must clearly state their permitted uses, rights, and obligations related to shared data to ensure compliance with CDPA Sections 13 and 28, and to protect data subjects' rights.

Procedures must be implemented to manage data subject requests and institutional data rights agreements in a timely, documented, and auditable manner.

8. DATA TRANSFERS

Where research collaborations necessitate data transfer outside Zimbabwe:

- An assessment of the destination country's data protection adequacy must be conducted as required by CDPA Section 28;
- Data transfer agreements must include contractual clauses ensuring equivalent or stronger data protection measures;
- Any cross-border transfer requires written approval from the BRTI-THRUZIM DMD, DPO and must be documented;
- BRTI-THRUZIM prioritises the sharing of anonymised or de-identified datasets to minimise risk.

9. DATA BREACH MANAGEMENT

A data breach includes any unauthorised access, disclosure, alteration, loss, or destruction of personal data. In such events:

- The DPO must be informed immediately;
- An internal investigation will be initiated and documented;
- A breach notification must be submitted to the Data Protection Authority within 24 hours (Section 19);
- Corrective action and communication plans will be implemented, including informing affected participants where necessary.

10. DATA RETENTION AND DESTRUCTION

Retention periods must be determined during the ethics and protocol development stages. At a minimum:

- Data must be retained for 10 years, or longer if required by funders, journals, or national regulations;
- Secure deletion or physical destruction (e.g., shredding, digital wiping) must be used for disposal;
- Confirmation of destruction must be submitted to the BRTI-THRUZIM Research DMD, DPO and may be audited.

11. ROLES AND RESPONSIBILITIES

- Ensure that research data are collected, recorded, and managed in accordance with this policy and relevant guidelines.
- Develop and implement data management plans for all research projects, outlining procedures for data collection, storage, backup, sharing, and long-term preservation.
- Document research data comprehensively, including methodologies, protocols, instruments, and any associated metadata necessary for data interpretation and reuse.
- Safeguard the confidentiality, integrity, and security of research data throughout the data lifecycle.
- Ensure compliance with legal and ethical standards, institutional policies, and funder requirements related to research data management.
- Facilitate data sharing and collaboration where appropriate, while respecting intellectual property rights, privacy, and confidentiality.

12. ADDITIONAL OPERATIONAL OBLIGATIONS

All research projects conducted under BRTI-THRUZIM must have a Data Management Plan (DMP) developed and approved prior to the start of data collection. The DMP must comply with the requirements of the Cyber and Data Protection Act [Chapter 12:07] and institutional policies, ensuring that data processing is lawful, secure, and auditable.

12.1 Data Management Plan (DMP) Requirements

Researchers must:

- Identify the lawful grounds for data processing in line with CDPA Section 17 and document the legal basis and consent procedures (CDPA Section 13).
- Clearly define data collection methods, variables, and units of analysis to maintain consistency and accuracy.
- Use standardized formats, protocols, and instruments to support data interoperability and integration.
- Record all necessary metadata to facilitate data interpretation, replication, and validation.
- Specify retention periods, secure access protocols, and backup procedures, ensuring only authorised personnel can access personal or sensitive data (CDPA Section 18(4)).

13. POLICY ENFORCEMENT AND REVIEW

Non-compliance with this policy may result in:

- Disciplinary action for staff and students;
- Suspension or termination of data access;
- Notification to ethics committees or regulatory authorities.

This policy will be reviewed every two years or sooner if required by law, institutional policy changes, or emerging risks.

For questions or concerns regarding this policy, contact the DMD and DPO at:
tbandason@brti.co.zw | tnyengerai@brti.co.zw