Mycetoma Research Center | WHO Collaborating Center on Mycetoma

Excellence and Leadership

www.mycetoma.edu.sd
info@mycetoma.edu.sd

Strategy and Standard Operating Procedures for Managing Patients' Data and Records for Clinical and Scientific Research

Section 1: Overall Strategy

Vision

To establish a secure, ethical, and efficient data governance system that ensures the protection, accuracy, and accessibility of patient data for clinical care, research, and public health decision-making, while meeting international standards and local regulatory requirements.

Mission

To safeguard patient confidentiality, improve data integrity, and facilitate high-quality clinical and scientific research that contributes to a better understanding, prevention, and management of mycetoma.

Strategic Objectives

1. **Strengthen Data Governance**
    - Implement a unified data management policy aligned with national and international ethical standards.
    - Establish clear ownership, access control, and accountability mechanisms.

2. **Ensure Data Quality and Integrity**
    - Standardise data collection tools, digital systems, and verification processes.

- Conduct routine validation, audits, and quality checks.

3. **Enhance Data Security and Confidentiality**
   - Implement secure digital infrastructure, including encryption and access controls.
   - Train staff on data protection and privacy regulations.

4. **Facilitate Ethical and Responsible Data Use**
   - Ensure informed consent, transparency, and oversight for research use.
   - Implement clear procedures for data sharing, collaborations, and publications.

5. **Support Research and Innovation**
   - Provide researchers with high-quality, anonymised datasets.
   - Promote responsible open science while protecting patient rights.

Section 2: Data Governance Structure

Data Governance Committee (DGC)

A standing committee responsible for oversight of all clinical and research data.

Composition:

- Director, MRC (Chair)
- Head of Clinical Services
- Head of Research and Scientific Affairs
- Data Manager
- Legal/Ethics officer
- IT Systems Administrator
- External advisor

Functions:

- Approve data access requests
- Review ethical and legal compliance
- Oversee data security and audits
- Approve data-sharing agreements
- Resolve disputes related to data usage

Section 3: Standard Operating Procedures (SOPs)

SOP 1: Data Collection

Purpose

To ensure standardised, accurate, and ethically compliant collection of patient data.

Scope

All clinical, demographic, diagnostic, imaging, laboratory, and follow-up data were collected from patients at MRC.

Procedures

Before Data Collection

1. Verify that the patient has signed **informed consent** (clinical + research).
2. Assign a **unique patient identification code (PID)**; no names should appear in data forms used for research.
3. Ensure all staff collecting data are trained in GCP (Good Clinical Practice).

During Data Collection

Use standardised tools:

- Electronic Medical Record system (EMR)
- Structured Case Report Forms (CRFs)
- Laboratory data sheets
- Radiology/ultrasound reporting templates

Data must include:

- Demographics
- Clinical presentation
- Diagnostic results (lab, histopathology, imaging)
- Treatment regimen
- Follow-up assessments

After Data Collection

1. Data is recorded **immediately** or within 24 hours.
2. Supervisors perform cross-checks for errors or omissions.
3. Data is submitted to the Data Manager for validation and integration into the master database.

SOP 2: Data Storage and Security

Purpose

To protect patient confidentiality and preserve data integrity.

Procedures

Physical Data (Paper Records)

1. Stored in locked cabinets in restricted-access rooms.
2. Access is given only to authorised clinicians, data managers, and auditors.
3. Records must never be removed from MRC without approval.

Electronic Data

1. Stored in a secure, encrypted server on-site at MRC.
2. Daily automated backups are stored in an off-site secure location.
3. Implement access control using:
   - Usernames
   - Passwords
   - Two-factor authentication (for sensitive datasets)

All data transmissions must use encrypted channels (SSL/TLS).

SOP 3: Data Entry, Cleaning, and Validation

Purpose

To ensure accurate and consistent digitisation of patient data.

Procedures

1. Data Entry Officers enter data into the EMR or research database within 48 hours.
2. Data Manager conducts:
    - Completeness checks
    - Logical consistency checks
    - Cross-validation with source documents
3. Errors are documented, corrected, and logged.
4. DGC or an external reviewer conducts monthly quality audits.

SOP 4: Data Access and Use for Clinical Care

Purpose

To ensure patient data is used appropriately to support medical care.

Procedures

1. Clinicians can access identifiable patient data only for direct care.
2. Access is granted through authorised accounts.
3. Any printouts must be labeled **CONFIDENTIAL** and securely stored.

SOP 5: Data Use for Scientific Research

Purpose

To support high-quality research while protecting patient rights.

Procedures

Research Proposals

Researchers submit:

1. Research proposal
2. Data request form
3. Ethical approval certificate
4. Data protection plan

DGC reviews and approves access.

Data Preparation

1. Data Manager provides **anonymised or pseudonymised datasets**.
2. Direct identifiers (name, address, phone, ID number) are removed.
3. Limited datasets may be provided under strict conditions for longitudinal studies.

Data Usage Rules

1. Data must be used only for the approved study.
2. No re-identification attempts.
3. No sharing with unauthorised persons.
4. Publications must acknowledge MRC.

SOP 6: Data Sharing and External Collaborations

Purpose

To guide ethical and secure data sharing with collaborators.

Required Documents

- Data Sharing Agreement (DSA)
- Material Transfer Agreement (MTA) (if applicable)
- Ethics approval from the collaborating institution

Procedures

- Only anonymised data shared.
- Shared using secure, encrypted transfer portals only.
- External parties must commit to:
- Not re-identify patients
- Use data only for agreed purposes
- Delete data after project completion (unless otherwise agreed)

SOP 7: Data Retention and Archiving

Procedures

- Clinical records are retained for at least 10 years.
- Research data is retained for 5 years after publication.
- Archived data is stored in secure digital and physical repositories.
- After the retention period, data may be:
    - Permanently archived
    - De-identified for teaching
    - Destroyed securely (shredding or digital wiping)

SOP 8: Data Breach Management

Procedures

1. Immediately report breach to:
    - Director, MRC
    - Data Governance Committee
    - University legal office
2. Investigate within 72 hours.
3. Take corrective actions:
    - Isolate compromised systems
    - Reset access codes
    - Strengthen security protocols
4. Notify affected individuals if required.
5. Document breach and lessons learned.

SOP 9: Staff Training and Compliance

Procedures

1. All staff handling data must complete:
   - GCP Training
   - Data Protection and Privacy Training
   - Research Ethics Training
2. Training is refreshed every 2 years.
3. Non-compliance leads to disciplinary action.

Section 4: Expected Outcomes

- Improved patient confidentiality and trust
- Higher-quality clinical and research data
- Stronger compliance with ethics and regulations
- Enhanced capacity for international research collaborations
- Improved evidence-based decision-making
- Sustainable institutional data governance

Approval:

The Mycetoma Research Centre Director approved

these policies and Standard Operating Procedures

23rd June 2021