# HE²AT Center Data Management Plan v2.2 - Cloud Migration Changes Summary

## Document Overview

* **Document**: NIH HE²AT Center Data Management Plan
* **Version**: 2.2 (Cloud Migration Update)
* **Previous Version**: 2.1 (September 2024)
* **Update Date**: August 2025
* **Primary Change**: Migration from UCT on-premise servers to WHC-managed cloud infrastructure
* **Ethics Review Status**: Submitted to Wits HREC for review and approval
* **HREC Reference Numbers**: RP1 (220605), RP2 (220606)

## Summary of Changes Table

| Section | Change Type | Description | Rationale |
| --- | --- | --- | --- |
| **4.1.2 Data Storage Infrastructure** | Addition | Added cloud storage infrastructure alongside existing UCT servers | Dual capability during transition period |
| **4.2 Data Security** | Enhancement | Enhanced security measures including zero-trust architecture and SOC monitoring | Cloud-specific security requirements |
| **6.1 Data Access and Sharing** | Update | Updated access protocols to include cloud-based authentication systems | Maintain security in cloud environment |
| **6.4 Data Transfer Protocols** | Addition | New protocols for secure cloud data transfer using AES-256 encryption | Ensure secure migration process |
| **8 Data Preservation** | Enhancement | Added cloud-based preservation strategies with geographic redundancy | Improved data resilience and availability |
| **14.1 Data Management Roles** | Update | Clarified roles for cloud infrastructure management | Clear accountability in new environment |
| **14.2 Training Requirements** | Addition | Added cloud platform training requirements for staff | Ensure competency in new systems |
| **14.3 Compliance Monitoring** | Enhancement | Enhanced monitoring for cloud compliance with POPIA and international standards | Maintain regulatory compliance |
| **17 Cloud Migration Implementation** | New Section | Comprehensive cloud migration implementation plan | Document migration strategy and timeline |
| **Ethics and HREC Compliance** | Update | Updated procedures for ongoing HREC notification during cloud migration | Ensure continued ethics compliance during infrastructure changes |

## Key Infrastructure Changes

| Component | Version 2.1 (Before) | Version 2.2 (After) | Impact |
| --- | --- | --- | --- |
| **Primary Storage** | UCT on-premise servers | WHC-managed cloud + UCT (dual capability) | Improved scalability and reliability |
| **Data Access** | On-premise authentication | Cloud-based identity management + existing systems | Enhanced access control |
| **Security Monitoring** | Standard monitoring | SOC monitoring + zero-trust architecture | Proactive threat detection |
| **Backup Strategy** | Local backups | Geographic redundancy across cloud regions | Enhanced disaster recovery |
| **Encryption** | Standard encryption | AES-256 encryption for data in transit and at rest | Strengthened data protection |

## Data Categories Affected

| Data Type | Migration Impact | Timeline | Special Considerations |
| --- | --- | --- | --- |
| **Original Study Data** | Gradual migration with validation | Months 1-6 | Requires extensive validation protocols |
| **Consortium Shared Data** | Priority migration | Months 2-4 | Collaboration tools integration needed |
| **De-identified Data** | Standard migration | Months 3-8 | Analytics platform compatibility |
| **Inferential Data** | Phased migration | Months 4-10 | Model deployment considerations |

## Compliance and Governance Changes

| Aspect | Enhancement | Implementation |
| --- | --- | --- |
| **POPIA Compliance** | Cloud-specific privacy controls | Regular audits and assessments |
| **Data Governance** | Enhanced cloud governance framework | Updated policies and procedures |
| **Access Controls** | Multi-factor authentication | Phased rollout to all users |
| **Audit Trails** | Enhanced logging and monitoring | Real-time compliance tracking |

## Implementation Timeline

| Phase | Duration | Key Activities | Deliverables |
| --- | --- | --- | --- |
| **Phase 1: Planning** | Months 1-2 | Infrastructure setup, policy updates | Cloud environment ready |
| **Phase 2: Pilot Migration** | Months 2-4 | Test data migration, validate processes | Pilot validation complete |
| **Phase 3: Full Migration** | Months 4-8 | Migrate all data categories | All data in cloud |
| **Phase 4: Optimisation** | Months 8-10 | Performance tuning, process refinement | Optimised operations |

## Risk Mitigation

| Risk | Mitigation Strategy | Monitoring |
| --- | --- | --- |
| **Data Loss** | Dual storage during transition | Continuous validation |
| **Security Breach** | Zero-trust architecture | 24/7 SOC monitoring |
| **Compliance Gaps** | Regular compliance assessments | Monthly reviews |
| **Performance Issues** | Gradual migration approach | Performance metrics tracking |

## Training and Support

| Stakeholder Group | Training Requirements | Timeline |
| --- | --- | --- |
| **Data Managers** | Cloud platform administration | Month 1 |
| **Researchers** | New access procedures | Month 2 |
| **IT Support** | Cloud infrastructure management | Month 1-2 |
| **Compliance Team** | Cloud governance and auditing | Month 2-3 |

## Ethics Review Considerations for Wits HREC

### Changes Requiring HREC Notification

| Change Category | Specific Updates | Ethics Implications | HREC Action Required |
| --- | --- | --- | --- |
| **Data Storage Infrastructure** | Migration to WHC-managed cloud infrastructure | Changes to data storage location and security architecture | Notification of infrastructure changes |
| **Data Security Enhancements** | Implementation of AES-256 encryption and SOC monitoring | Enhanced protection of participant data | Review of updated security measures |
| **Access Control Updates** | Cloud-based authentication and multi-factor authentication | Changes to data access procedures | Review of updated access protocols |
| **Cross-border Data Considerations** | Potential cloud storage across geographic regions | May involve cross-border data transfer | Assessment of international data protection compliance |
| **Data Processing Locations** | Distributed cloud processing capabilities | Changes to where data processing occurs | Review of processing location implications |

### Ethical Safeguards Maintained

| Safeguard | v2.1 Implementation | v2.2 Enhancement | Compliance Status |
| --- | --- | --- | --- |
| **Data De-identification** | Standard de-identification procedures | Enhanced automated de-identification with cloud tools | Maintained and improved |
| **Consent Compliance** | Original consent parameters respected | Same consent framework with enhanced security | Fully maintained |
| **POPIA Compliance** | Basic POPIA adherence | Enhanced POPIA compliance with automated monitoring | Strengthened |
| **Access Restrictions** | Role-based access control | Enhanced role-based access with MFA and audit trails | Improved |
| **Data Retention Policies** | Standard retention periods | Same periods with improved backup/recovery | Maintained with enhanced reliability |

### Risk Mitigation for Ethics Concerns

| Potential Risk | Mitigation Strategy | Monitoring Approach | HREC Oversight |
| --- | --- | --- | --- |
| **Data Security Breaches** | Zero-trust architecture and 24/7 SOC monitoring | Real-time threat detection and automated alerts | Quarterly security reports to HREC |
| **Unauthorized Access** | Multi-factor authentication and enhanced access controls | Comprehensive audit logging and access reviews | Annual access review reports |
| **Cross-border Data Transfer** | Compliance with international data protection standards | Automated compliance monitoring and reporting | Regular compliance status updates |
| **Data Loss/Corruption** | Geographic redundancy and automated backup systems | Continuous data integrity monitoring | Incident reporting procedures |

### Implementation Timeline for Ethics Compliance

| Phase | Duration | Key Ethics Activities | HREC Engagement |
| --- | --- | --- | --- |
| **Phase 1: Planning** | Months 1-2 | Ethics impact assessment, policy updates | Initial HREC notification of planned changes |
| **Phase 2: Pilot Migration** | Months 2-4 | Ethics compliance testing, security validation | Progress update to HREC with pilot results |
| **Phase 3: Full Migration** | Months 4-8 | Ongoing ethics monitoring during migration | Mid-migration compliance report |
| **Phase 4: Optimization** | Months 8-10 | Final ethics compliance verification | Final implementation report to HREC |

### Ongoing HREC Reporting Requirements

| Report Type | Frequency | Content | Purpose |
| --- | --- | --- | --- |
| **Migration Progress Reports** | Monthly during migration | Infrastructure changes, security updates, compliance status | Keep HREC informed of implementation progress |
| **Security Incident Reports** | As required | Any security incidents, breaches, or concerns | Ensure immediate HREC awareness of issues |
| **Compliance Status Reports** | Quarterly | POPIA compliance, international standards adherence | Demonstrate ongoing regulatory compliance |
| **Annual Review Report** | Annually | Comprehensive review of cloud implementation ethics impact | Annual ethics compliance assessment |

**HREC Submission Requirements:** - Updated Data Management Plan (v2.2) - Risk assessment for cloud migration - Security enhancement documentation - Compliance monitoring procedures - Staff training records for new systems

**Contact for HREC Queries:** - **Primary Contact**: Craig Parker (Craig.parker@witsphr.org) - **Data Management Lead**: Christopher Jack (cjack@csag.uct.ac.za) - **Ethics Compliance Officer**: [To be designated]

**Note**: All changes maintain backward compatibility and dual capability during the transition period to ensure continuity of research operations whilst migrating to the cloud infrastructure. Enhanced ethics safeguards have been implemented throughout the migration process to ensure participant protection exceeds previous standards.