Attention# 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 | Specific Change | Ethics Relevance |
| --- | --- | --- | --- |
| **4.1.2 Original Study Data Storage** | Enhancement | Added WHC-managed cloud infrastructure with AES-256 encryption alongside UCT servers | Enhanced data security and POPIA compliance |
| **4.2 Climate Data Storage** | Addition | WHC-managed cloud services with auto-scaling capabilities | Improved data accessibility for researchers |
| **6.1 Data Pre-processing Infrastructure** | Enhancement | WHC-managed cloud infrastructure with enhanced security and automated backup systems | Strengthened data protection measures |
| **6.4 Database Population** | Enhancement | Cloud-native database services with automated backup and enhanced data integrity | Improved data reliability and disaster recovery |
| **8 Data Analysis Platform** | Addition | Cloud-based computational resources with GPU acceleration | Enhanced analytical capabilities while maintaining security |
| **14.1 Data Transfer and Storage** | Enhancement | AES-256 encryption standard for both UCT servers and cloud storage | Strengthened encryption for participant data protection |
| **14.2 Network Security** | Enhancement | WHC-managed cloud security with 24/7 SOC monitoring and advanced threat detection | Proactive security monitoring and incident response |
| **14.2 Firewall Protection** | Addition | Cloud-native firewall services alongside UCT’s Cisco firewall | Dual-layer security protection |
| **14.3 Authentication and Authorization** | Enhancement | Cloud-specific access controls and automated compliance reporting | Improved access control and audit capabilities |
| **17 Cloud Migration Implementation** | New Section | Complete 5-phase cloud migration strategy with risk mitigation | Systematic approach ensuring ethical compliance throughout migration |

## 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 Summary for Wits HREC

### Key Changes Requiring HREC Awareness

| Change | Description | Ethics Impact |
| --- | --- | --- |
| **Enhanced Data Storage** | Addition of WHC-managed cloud infrastructure with AES-256 encryption | **Improved participant data protection** - stronger encryption and security |
| **Dual Infrastructure** | Maintaining UCT servers alongside new cloud services | **Continuity assurance** - no disruption to existing protections |
| **Enhanced Security Monitoring** | 24/7 Security Operations Centre (SOC) monitoring and threat detection | **Proactive risk management** - immediate response to potential issues |
| **Automated Backup Systems** | Cloud-native backup and disaster recovery capabilities | **Data integrity protection** - enhanced protection against data loss |
| **Advanced Access Controls** | Cloud-specific access controls with automated compliance reporting | **Strengthened access management** - better audit trails and monitoring |

### Ethics Compliance Status

| Requirement | v2.1 Status | v2.2 Status | Change Impact |
| --- | --- | --- | --- |
| **POPIA Compliance** | Compliant | **Enhanced** | Stronger encryption and monitoring improve compliance |
| **Data De-identification** | Standard procedures | **Maintained** | Same procedures with enhanced security infrastructure |
| **Consent Requirements** | Fully respected | **Maintained** | No changes to consent framework |
| **Access Restrictions** | Role-based control | **Strengthened** | Enhanced with cloud-specific controls and audit trails |
| **Data Retention** | Policy compliant | **Improved** | Same periods with better backup and recovery |

### Risk Management Improvements

| Risk Area | Previous Mitigation | Enhanced Mitigation |
| --- | --- | --- |
| **Data Breaches** | Standard security measures | 24/7 SOC monitoring with real-time threat detection |
| **Unauthorized Access** | Role-based access control | Enhanced access controls with automated compliance reporting |
| **Data Loss** | Regular backups | Automated backup systems with geographic redundancy |
| **System Failures** | Standard disaster recovery | Cloud-native disaster recovery with enhanced capabilities |

**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.