**WITS HUMAN RESEARCH ETHICS COMMITTEE (MEDICAL)  
AMENDMENT NOTIFICATION  
HE²AT CENTRE DATA MANAGEMENT PLAN VERSION 2.2**

**Document Title:** NIH HE²AT Centre Data Management Plan - Cloud Migration Amendment

**Version:** 2.2 (Cloud Migration Update)

**Previous Version:** 2.1 (September 2024)

**Amendment Date:** August 2025

**HREC Reference Numbers:** RP1 (220605), RP2 (220606)

**Principal Investigators:**  Matthew Chersich (Wits PHR)

**Contact:** Craig Parker (Craig.parker@witsphr.org)

**NATURE OF AMENDMENT:** Infrastructure enhancement to include cloud-based data management alongside existing on-premise servers. This amendment introduces WHC-managed cloud infrastructure to improve data security, scalability, and disaster recovery capabilities whilst maintaining all existing ethical safeguards.

**PARTICIPANT IMPACT:** No direct impact on participants. Enhanced data protection measures only.

**RISK ASSESSMENT:** Risk reduced through enhanced security and backup capabilities.

**1. SUMMARY OF CHANGES**

The HE²AT Centre Data Management Plan has been updated to incorporate cloud infrastructure alongside existing UCT on-premise servers. This dual-capability approach enhances data security and operational efficiency whilst maintaining continuity of research operations.

**1.1 Key Changes Requiring HREC Approval**

| **Change Category** | **Description** | **Ethics Impact** |
| --- | --- | --- |
| Data Storage Infrastructure | Addition of WHC-managed cloud storage with AES-256 encryption alongside existing UCT servers | Enhanced participant data protection through stronger encryption and redundancy |
| Security Monitoring | Implementation of 24/7 Security Operations Centre (SOC) monitoring with automated threat detection | Proactive risk management and immediate response to potential security issues |
| Backup Systems | Geographic redundancy across multiple cloud regions with automated backup | Significantly reduced risk of data loss |
| Access Controls | Cloud-specific access controls with automated compliance reporting | Enhanced audit trails and monitoring of data access |
| Disaster Recovery | Cloud-native disaster recovery capabilities | Improved data integrity and availability |

**2. DETAILED CHANGES BY SECTION**

| **DMP Section** | **Subsection** | **Specific Change** | **Justification** |
| --- | --- | --- | --- |
| 4.1.2 | Original Study Data Storage | Added: WHC-managed cloud infrastructure with AES-256 encryption | Enhanced security and POPIA compliance |
| 4.2 | Climate Data Storage | Added: WHC cloud services with auto-scaling | Improved data accessibility for researchers |
| 6.1 | Data Pre-processing | Added: Cloud infrastructure with automated backup | Strengthened data protection measures |
| 6.4 | Database Population | Added: Cloud-native database services | Improved reliability and disaster recovery |
| 8 | Data Analysis Platform | Added: Cloud computational resources with GPU | Enhanced analytical capabilities |
| 14.1 | Data Encryption | Specified: AES-256 encryption standard | Strengthened encryption standards |
| 14.2 | Network Security | Added: 24/7 SOC monitoring and cloud firewall | Proactive security monitoring |
| 14.3 | Access Controls | Added: Cloud-specific controls with reporting | Improved access management |
| 17 | Cloud Migration | New section: 5-phase migration strategy | Systematic implementation approach |

**3. INFRASTRUCTURE COMPARISON**

| **Component** | **Version 2.1 (Previous)** | **Version 2.2 (Current)** | **Improvement** |
| --- | --- | --- | --- |
| Primary Storage | UCT on-premise servers only | UCT servers + WHC cloud (dual) | Redundancy and scalability |
| Encryption | Standard encryption | AES-256 encryption specified | Industry-leading encryption |
| Monitoring | Standard monitoring | 24/7 SOC monitoring | Continuous security oversight |
| Backup | Local backups | Geographic redundancy | Enhanced disaster recovery |
| Firewall | UCT Cisco firewall | UCT + cloud-native firewall | Dual-layer protection |
| Authentication | UCT protocols | UCT + cloud controls | Enhanced access control |

**4. IMPLEMENTATION TIMELINE**

| **Phase** | **Duration** | **Key Activities** | **Risk Mitigation** |
| --- | --- | --- | --- |
| Phase 1: Planning | Months 1-2 | Infrastructure setup, policy updates, staff training | Comprehensive risk assessment completed |
| Phase 2: Pilot | Months 2-4 | Test migration with validation | Limited scope reduces risk |
| Phase 3: Migration | Months 4-8 | Phased data migration | Dual systems ensure continuity |
| Phase 4: Completion | Months 8-10 | Full migration and validation | Extensive testing before cutover |
| Phase 5: Optimisation | Months 8-10 | Performance tuning | Continuous monitoring |

**5. DATA CATEGORIES AND MIGRATION**

| **Data Type** | **Sensitivity Level** | **Migration Timeline** | **Special Protections** |
| --- | --- | --- | --- |
| Original Study Data | Highly Sensitive | Months 1-6 | Requires provider approval; extensive validation |
| Consortium Shared Data | Sensitive | Months 2-4 | Limited access; collaboration tools integration |
| De-identified Data | Moderate | Months 3-8 | Analytics platform compatibility required |
| Inferential Data | Low | Months 4-10 | Aggregated data; no individual identifiers |

**6. SECURITY ENHANCEMENTS**

| **Security Layer** | **Enhancement** | **Benefit to Participant Protection** |
| --- | --- | --- |
| Encryption | AES-256 for data at rest and in transit | Military-grade encryption protects all participant data |
| Access Control | Multi-factor authentication required | Prevents unauthorised access to participant data |
| Monitoring | 24/7 SOC with real-time alerts | Immediate detection and response to threats |
| Architecture | Zero-trust security model | No implicit trust; continuous verification |
| Audit Trails | Automated logging and reporting | Complete record of all data access |
| Backup | Geographic redundancy | Protection against data loss from disasters |

**7. COMPLIANCE STATUS**

| **Requirement** | **Version 2.1 Status** | **Version 2.2 Status** | **Change Impact** |
| --- | --- | --- | --- |
| POPIA Compliance | Compliant | Enhanced Compliance | Stronger encryption and monitoring |
| Data De-identification | Standard procedures | Maintained | Same procedures; enhanced infrastructure |
| Consent Framework | Fully implemented | Unchanged | No changes to consent requirements |
| Access Restrictions | Role-based control | Enhanced controls | Cloud-specific controls added |
| Data Retention | Policy compliant | Improved capability | Better backup and recovery |
| Audit Capability | Manual processes | Automated | Real-time compliance tracking |

**8. TRAINING AND SUPPORT**

| **Stakeholder Group** | **Training Requirements** | **Timeline** | **Status** |
| --- | --- | --- | --- |
| Data Managers | Cloud platform administration | Month 1 | Scheduled |
| Researchers | New access procedures | Month 2 | Materials prepared |
| IT Support | Cloud infrastructure management | Months 1-2 | In progress |
| Compliance Team | Cloud governance and auditing | Months 2-3 | Planned |

**9 ETHICAL CONSIDERATIONS**

**9.1 Participant Protection**

* No changes to the consent framework or participant rights
* Enhanced data protection through stronger encryption
* Improved security monitoring reduces the risk of data breaches
* Geographic redundancy protects against data loss

**9.2 Data Governance**

* Maintained compliance with all existing ethical guidelines
* Enhanced audit trails improve accountability
* Automated compliance reporting ensures ongoing adherence
* No changes to data access restrictions or approval processes

**9.3 Transparency**

* Clear documentation of all infrastructure changes
* Regular reporting to HREC on migration progress
* Open communication with data providers about changes
* Maintenance of all existing oversight mechanisms

**10. DECLARATIONS AND ASSURANCES**

**We hereby declare that:**

* All changes maintain or enhance existing ethical safeguards
* No changes compromise participant privacy or data security
* The migration will be conducted with continuous risk assessment
* Dual capability ensures no disruption to research activities
* All staff will be appropriately trained before accessing cloud systems
* Regular audits will verify compliance throughout the migration
* Any issues identified will be immediately reported to HREC

**11. CONCLUSION**

The version 2.2 amendments to the HE²AT Centre Data Management Plan represent infrastructure enhancements that strengthen data protection whilst maintaining all existing ethical safeguards. The addition of cloud infrastructure provides improved security, scalability, and disaster recovery capabilities without changing any consent frameworks, data de-identification procedures, or participant rights.

The phased migration approach with dual capability ensures continuity of research operations whilst implementing these enhancements. All changes have been designed to exceed previous security standards and provide additional protection for participant data.

**HREC ACTION REQUESTED:** Review and approval of the Data Management Plan version 2.2 amendments, specifically the addition of WHC-managed cloud infrastructure to enhance data security and operational capabilities.

**TIMELINE:** Implementation to begin upon HREC approval, with completion within 10 months.

**MONITORING:** Quarterly progress reports will be submitted to HREC throughout the migration period.

**CONTACT INFORMATION**

| **Role** | **Name** | **Email** | **Phone** |
| --- | --- | --- | --- |
| Primary Contact | Craig Parker | Craig.parker@witsphr.org | [Phone Number] |
| Data Management Lead | Christopher Jack | cjack@csag.uct.ac.za | [Phone Number] |
| Ethics Compliance Officer | [To be designated] | [Email] | [Phone Number] |

**ATTACHMENTS**

* ☐ Complete Data Management Plan Version 2.2
* ☐ Cloud Infrastructure Technical Specifications

**Document Version:** 2.2  
**Date:** August 2025  
**Prepared by:** HE²AT Centre Data Management Team