# 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

## 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 |

## 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 |

**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.