MiHealth Health Portal - Service Definition Document

1. Executive Summary

MiHealth Health Portal offers a secure, cloud-hosted platform for receiving remote blood-pressure monitoring readings; height and weight; BMI; and further extends to patient facing services, including appointment system arrival and health promotion; secure clinical data capture via configurable in-context patient questionnaire.

Device readings from compatible devices and patient initiated health data is passed into the Portal for clinical validation, supporting seamless integration and scalable digital care.

2. Service Overview

2.1 Service Description

The Health Portal functions as a central data repository and clinical management platform for proactive health monitoring data and health promotion questionnaire data. Compatible blood pressure monitors act purely as input devices, transmitting readings to the cloud platform. Clinicians access the portal through web browsers or mobile devices to review patient data, configure alert thresholds, and make clinical decisions based on longitudinal trend analysis.

2.2 Target Users

Primary users include:

- GP practices and primary care networks managing hypertensive patients
- Community health teams providing chronic disease management services
- Hospital discharge teams requiring post-discharge monitoring capabilities
- Specialist hypertension clinics and cardiology departments
- Integrated care systems implementing population health management programmes

3. Technical Architecture

3.1 Infrastructure

The platform operates on Microsoft Azure cloud infrastructure within UK regions, ensuring data sovereignty and compliance with NHS data residency requirements. The architecture employs Azure's Platform-as-a-Service (PaaS) offerings including App Service, Azure SQL Database, Azure Storage, and Azure API Management. Multi-zone deployment across availability zones provides resilience against datacenter-level failures. All components leverage Azure's native security features including DDoS protection, Web Application Firewall, and Azure Security Centre monitoring.

3.2 Application Architecture

Microservices architecture separates concerns into independently deployable components: data ingestion service (receives readings from monitors), clinical rules engine (evaluates thresholds and generates alerts), notification service (sends alerts via email/SMS), reporting service (generates analytics), and API gateway (manages internal Microtech integrations). This design enables independent scaling, isolated fault domains, and technology stack flexibility. Service-to-service communication utilizes Azure Service Bus for asynchronous messaging and Azure API Management for synchronous REST calls.

3.3 Data Storage

Patient data resides in Azure SQL Database with Transparent Data Encryption (TDE) enabled. Database configured for geo-redundant backup with 30-day point-in-time restore capability. Hot data (recent 90 days) stored in primary database tables, older data archived to Azure Blob Storage with lifecycle policies. Binary content (uploaded documents, exported reports) stored in Azure Blob Storage with encryption at rest. All storage accounts configured for geo-redundant storage (GRS) with replication to secondary UK region.

3.4 Integration Architecture

Pre-built connectors available for EMIS Web, TPP SystmOne, and Vision GP systems utilising vendor-specific APIs where FHIR not yet available. Integration patterns support: patient demographic synchronisation (ensuring consistent patient identification), and appointment book data.

4. Security and Compliance

4.1 Information Security Management

ISO 27001:2022 certified Information Security Management System (ISMS) governs all security practices. Annual surveillance audits by accredited certification body verify ongoing compliance. Information security policies cover: access control, asset management, cryptography, physical security, operations security, communications security, system acquisition and development, supplier relationships, incident management, business continuity, and compliance. Policy framework reviewed annually and updated following significant incidents or regulatory changes. All staff undergo security awareness training during induction and annually thereafter.

4.2 Data Protection and Privacy

GDPR compliance maintained through comprehensive data protection framework including: lawful basis documentation (Article 6 and 9 processing), Data Protection Impact Assessments (DPIA) for high-risk processing, Records of Processing Activities (ROPA), data subject rights procedures (access, rectification, erasure, portability), breach notification processes, and data retention policies. Data Processing Agreements provided to all customers documenting processor responsibilities. Dedicated Data Protection Officer oversees compliance program and serves as point of contact for supervisory authorities and data subjects.

4.3 Clinical Safety

DCB0129 and DCB0160 clinical risk management standards compliance ensures patient safety. Qualified Clinical Safety Officer (registered healthcare professional with clinical safety training) appointed to oversee safety management system. Clinical Safety Case documentation includes: hazard identification and analysis, risk evaluation and mitigation, safety requirements specification, and residual risk assessment. Hazard log maintained documenting identified hazards, severity ratings, probability assessments, risk scores, mitigations, and residual risks. Safety incidents reported through dedicated pathway with investigation and learning process. Annual clinical safety review conducted with independent clinical safety assurance.

4.4 Penetration Testing

Annual penetration testing by CREST-approved cybersecurity firms identifies vulnerabilities before malicious actors can exploit them. Testing scope includes: external infrastructure testing, web application testing (OWASP Top 10), API security testing, and social engineering assessment. Tests conducted using industry-standard methodologies (OWASP Testing Guide, PTES). Findings classified by severity with remediation timelines: Critical (7 days), High (30 days), Medium (90 days). Remediation verification testing confirms effective fixes. Test reports provided to customers under NDA upon request during procurement evaluation.

4.5 NHS Data Security and Protection Toolkit

Annual Data Security and Protection Toolkit (DSPT) submission achieves 'Standards Met' status. Toolkit covers ten data security standards including: personal confidential data, staff responsibilities, training, managing data access, process reviews, responding to incidents, continuity planning, unsupported systems, IT protection, and accountable suppliers. Evidence library maintained demonstrating compliance with each mandatory assertion. Senior Information Risk Owner (SIRO) at board level provides executive oversight of information risk management.

5. Service Management

5.1 Service Level Agreement

99.9% uptime SLA calculated monthly permits maximum 43 minutes unplanned downtime per month. Availability measured using Microsoft Azure's monitoring infrastructure supplemented by independent third-party monitoring. Planned maintenance excluded from availability calculations when: 7 days advance notice provided, scheduled during low-usage periods (typically Sunday 2-6am), duration does not exceed 4 hours per occurrence

5.2 Incident Management

Standard Support (included in base price): email and phone support during business hours (8am-6pm Mon-Fri), response within 2 business hours for critical issues. Access to online knowledge base, video tutorials, and documentation P1 - Response time 2 hours; fix time 5 hours P2 - Response time 3 hours; fix time 7 hours P3 - Response time 5 hours; fix time 1.5 days P4 (RFI) - 10 days to completion

5.3 Change Management

Structured change management process balances innovation with stability. Change categories: Standard changes (pre-approved, low risk, automated deployment), Normal changes (requires Change Advisory Board approval, scheduled deployment window), Emergency changes (expedited approval for critical security patches or major incident resolution). All normal changes require: business justification, technical design, security impact assessment, rollback plan, test evidence, and CAB approval. Release schedule: minor updates deployed weekly during maintenance window, major releases quarterly with extended testing period, security patches deployed within 24-48 hours based on severity. Customers receive advance notification of changes via email and in-portal announcements.

5.4 Continuous Improvement

ISO 9001:2015 quality management system drives continuous service improvement. Customer feedback collected through: quarterly satisfaction surveys, user group meetings, support ticket analysis, and feature request portal. Product roadmap published quarterly showing planned enhancements and priorities. Service improvement register tracks identified opportunities with priority ranking and implementation status. Key performance indicators monitored monthly: user satisfaction scores, support ticket resolution times, system availability, feature adoption rates, and security metrics. Annual management review assesses quality management system effectiveness and identifies improvement opportunities.

6. Implementation Methodology

6.1 Implementation Approach

Comprehensive onboarding program ensures successful implementation. Process begins with kick-off meeting to understand requirements, clinical workflows, and technical environment. Implementation timeline includes technical setup including Azure tenant provisioning; user account creation, and role-based access configuration; configuration of clinical thresholds; patient cohort setup; device pairing; data migration (if applicable), and system testing; user training via combination of webinars and self-paced e-learning modules. Training covers: clinician use; administrative functions; patient onboarding; troubleshooting. Provide comprehensive documentation: user guides, quick reference cards, video tutorials, FAQ database. Assign dedicated implementation manager throughout onboarding. Post-go-live support includes 30-day enhanced support period with daily check-ins, troubleshooting assistance, and workflow optimisation. Patient engagement toolkit provided including information leaflets, posters, consent forms, and email templates. Implementation checklist ensures all steps completed before go-live.

6.2 Implementation for Larger Organisations

Multi-site implementations (Health Boards, Primary Care Networks, Community Trusts, ICS-wide deployments) follow adapted methodology with extended timelines. Additional activities include: stakeholder mapping and engagement across sites, technical architecture design for complex integration requirements, change management planning and communications, training-the-trainer program for local champions, phased site rollout with lessons learned incorporated, and governance structure establishment for ongoing service oversight.

7. Support Services

7.1 Standard Support (Included)

Standard Support (included in base price): email and phone support during business hours (8am-6pm Mon-Fri), response within 2 business hours for critical issues. Access to online knowledge base, video tutorials, and documentation P1 - Response time 2 hours; fix time 5 hours P2 - Response time 3 hours; fix time 7 hours P3 - Response time 5 hours; fix time 1.5 days P4 (RFI) - 10 days to completion

7.2 Knowledge Base and Self-Service

Comprehensive knowledge base containing: user guides for all roles (administrator, clinician, patient), quick start guides and video tutorials, frequently asked questions, troubleshooting guides, integration documentation, API reference documentation, and release notes. Content searchable and categorized by role and topic. Community forum enables peer-to-peer support and knowledge sharing. Monthly webinars covering new features and best practices. Quarterly user group meetings for larger customers.

7.3 Training Services

Standard implementation includes training for up to 10 users (remote sessions). Training modules: system administration, clinical user training, patient onboarding process. Train-the-trainer program for organisations wanting internal capability. E-learning modules available for self-paced learning and ongoing onboarding.

8. Terms and Conditions

8.1 Contract Terms

Minimum contract period: 12 months from go-live date. Contracts renew automatically for successive 12-month periods unless 90 days written notice provided by either party. No early termination fees after initial 12-month period completed. During initial 12 months, early termination permitted with 90 days notice plus payment of remaining contractual obligations. Price changes limited to annual increases capped at RPI.

8.2 Liabilities and Indemnities

Professional indemnity insurance: limit £2 million per claim. Public liability insurance: limit £10 million per claim. Product liability insurance: limit £10 million per claim. Insurance certificates provided upon request. Liability cap: total liability limited to 12 months' subscription fees except for: data breaches caused by our negligence, intellectual property infringement, fraud, or gross negligence (no cap). Force majeure provisions cover unforeseeable circumstances beyond reasonable control. Mutual indemnification for breach of respective obligations.

8.3 Data Ownership and Processing

Customer retains ownership of all patient data. We operate as data processor under GDPR Article 28, with customer as data controller. Data Processing Agreement documents: scope and purpose of processing, types of personal data, categories of data subjects, processor obligations, sub-processor arrangements, data security measures, breach notification procedures, data subject rights support, data deletion/return provisions, and audit rights. Customer determines lawful basis for processing. We process data solely according to customer instructions and contractual obligations.

8.4 Service Dependencies

Service requires: customer IT support for local connectivity issues, customer clinical governance oversight of monitoring program, patient consent for remote monitoring and data processing. Customer responsibilities: clinical decision-making based on data, appropriate clinical response to alerts, patient safety oversight, local clinical protocols, user account management. We provide technology platform but do not provide clinical services or replace clinical judgment.

9. Contact Information

Sales and Commercial Enquiries:

Email: sales@microtech-group.co.uk

Telephone: 01563 530 480

Web: www.microtech-group.co.uk

Technical Support:

Email: helpdesk@microtech-group.co.uk

Telephone: 01563 530 480