



Service Definition Statement SOP

v2 Approved on 2026-01-29

Table of Contents

- [Overview of my mhealth](#)
- [Background and Vision](#)
- [Product Benefits examples](#)
- [Implementation Plan](#)
- [Onboarding Support](#)
- [Digital Capabilities](#)
- [Pricing Structure](#)
- [Ordering and Invoicing Process](#)
- [Termination](#)
- [Technical Requirements](#)
- [Network and System Security](#)
- [Service Levels](#)
- [Data Management, Access, and Security](#)
- [Data backup, restore and disaster recovery](#)
- [Certifications/Aligned](#)
- [NICE Early Value Assessments\(EVAs\)](#)
- [Classification](#)

Uncontrolled when exported. Check version status before use. All times and dates are UTC.

Overview of my mhealth

The my mhealth application is a web-based platform developed by my mhealth Limited, comprising modular products including myCOPD, myHeart, myAsthma, and myDiabetes. Each module is designed to support patients in self-managing chronic conditions while enabling clinical teams to manage patient populations efficiently and at scale throughout the care pathway.

Aims:

Enhance Self-Management: my mhealth provides access to patients diagnosed with one or more of the supported chronic conditions (subject to contracted access), facilitating improved self-care outside of traditional clinical settings. The modules encourage patient engagement, adherence, and active participation in managing their health.

Improve Patient Outcomes: By educating and empowering patients, the platform aims to enhance outcomes and reduce the burden on healthcare resources. The self-management focus is supported by structured guidance, interactive tools, and personalised feedback within each module.

Enable New Models of Care: The platform supports clinical teams in delivering innovative care pathways at a



population level, using digital tools as an adjunct or alternative when face-to-face services are not feasible. This approach helps reduce inequalities in access to care while optimising patient engagement and supporting more flexible, technology-enabled models of healthcare delivery.

Generate and Utilise Evidence: my mhealth has a strong track record in research and evaluation, having secured grant funding from programmes such as SBRI and Innovate UK. Trials and evaluations provide evidence supporting the efficacy of the platform, with publications available on the supplier website.

Demonstrate Real-World Effectiveness: Data from routine use demonstrates outcomes comparable to standard cardiac and pulmonary rehabilitation programmes. Independent post-market surveillance shows high user satisfaction, ease of use, and positive recommendations from patients.

Healthcare System Engagement: my mhealth has achieved strong engagement across the NHS, with a growing and active user base each month. The platform aligns with the NHS Long Term Plan, which recognises digital health as essential to transforming care delivery, enabling self-management, and supporting scalable, sustainable healthcare models. This demonstrates the platform's relevance and contribution to both patients and clinical teams in delivering evidence-based, digitally enabled care.

Background and Vision

my mhealth was founded in 2011 to help people living with long-term conditions feel more informed, confident and in control of their health. Our digital tools are designed to support everyday self-management, putting practical, clinically grounded support into people's hands.

Everything we do is shaped by evidence. We have an active research community and work closely with clinicians, researchers and scientists to ensure our modules are grounded in the latest evidence and real-world learning. Our platform is secure, robust and continuously reviewed to meet high clinical and data standards.

my mhealth is widely used across the NHS, supporting both individuals and population-level health programmes. While our reach is national, our focus remains personal, creating tools that are simple to use, supportive and genuinely helpful in daily life.

Behind my mhealth is a dedicated team of clinicians, researchers, scientists, software specialists and an experienced support team who work together to deliver care at scale without losing what matters most, the person using our app.

Our purpose is clear. To improve health outcomes, support self-management and help people live well with their condition.

Product Benefits examples

For Patients:

- **Educational Videos:** Easy-to-follow videos such as inhaler technique to help patients manage their condition effectively.
- **Online Exercise Courses:** Complete courses such as pulmonary rehabilitation, Cardiac Rehabilitation and DM:Fit accessible from home.
- **Symptom Reporting:** Generate reports to track changes in symptoms over time.
- **Weather and Pollution Forecasting:** Receive daily forecasts to understand how local weather and air pollution may impact health, allowing for better planning.



- **Medication Reminders:** Notifications for medication reminders, updates from clinicians, or messages from the clinical team.
- **Medication Management:** View, add, and delete medications with prescription assessments based on national guidelines. Medications are condition-specific.
- **Self-Management Plan and Diary:** Detailed guidance on medication timing and usage, with a diary to record treatment adherence, visible in real-time on the clinical portal.
- **Guidance on App Usage:** Global guidance and how-to-use videos for each function within the app.
- **Shared Decision-Making Support:** Upload photos and information to aid in shared decision-making, such as diabetes eye, kidney, and foot care.
- **Walking Videos:** Follow-along walking videos of varying lengths to support at-home exercise.
- **Activity Diary:** Track physical and rehab activities, with the option to connect to integrated fitness devices via Bluetooth for seamless data capture.
- **In House UK based support team:** Available via WhatsApp messaging, phone or email
- **Unique and tailored evidence-based digital intervention** that's proven to improve health outcomes and reduce health service dependence

For Clinical Team Members:

- **Clinical Dashboard:** Deliver self-management, view reports and more- enhancing patient management.
- **Evidence-based rehabilitation:** Delivered to patients in the comfort of their own home - increasing capacity
- **Educational Videos:** Improve patients understanding and health using personalised and accredited education. Use videos, such as inhaler tutorials, for personal education updates or patient education during community or clinic visits.
- **Automated and customisable condition-specific care plans:** Patients recognise their symptoms and understands how to manage them
- **Medicine optimisation:** Help patients understand how and when to take their medication and improve adherence
- **Condition-specific interventions:** coping strategies, lifestyle advice and mental wellness pathways give patients more freedom
- **Product eLearning:** Available when it suits the individual or team

System Benefits:

- **Reducing Care Variations:** Standardised processes to minimise variations in care delivery.
- **Workforce Resilience:** Enhancing the capacity and resilience of healthcare teams.
- **Patient Support at Home:** Empowering patients to manage their health from home, reducing the need for frequent clinical visits.
- **myCOPD has been evaluated by NICE for delivery of pulmonary rehabilitation programmes for adults with COPD.** The outcome is a NICE recommendation for early use within the NHS until April 2027, while further evidence is gathered.
- **myCOPD has been evaluated by NICE to support self-management of COPD.** The outcome is a NICE recommendation for early use within the NHS until December 2027, while further evidence is gathered.
- **myHeart has been evaluated by NICE to support cardiac rehabilitation.** The outcome is a NICE recommendation for early use within the NHS until December 2028, while further evidence is gathered.
- **myAsthma NICE EVA draft published January 2026.** Recommends myAsthma as a Digital technology to support self-management of asthma.



Implementation Plan

In brief, our implementation plan *may* include:

- Working with stakeholders to understand the scope of the project and support necessary documentation, including a DPIA and a project initiation document.
- Stakeholder engagement, including but not limited to a kick-off meeting to plan and further scope the project, and facilitated pathway mapping sessions to understand the current clinical pathway, challenges, and opportunities for digital transformation.
- Account set up, we provide the initial set up via our operations team and hand this over when complete to reduce administrative burden.
- Training and support for clinical teams to implement the App, including launching new models of care and clinical pathways.
- Onboarding and engaging patients, this is facilitated by the Operations Team and can include supporting patients identified by clinicians during consultations, case load searches and remote activation where patients are contacted via SMS or letter and self-referrals via email and existing patient portals.
- Wider system engagement and remote activation, including working with stakeholders such as comms teams, social prescribers, pharmacy, digital inclusion teams, and patient groups to widen access and improve impact.
- Ongoing support from the Operations and Customer Success teams to continually review and refine the implementation
- Working with stakeholders to ascertain reporting requirements. These can be met by using the clinician interface to audit engagement or using our analytics platform to see real-time usage data and other metrics, this data can also be exported at agreed intervals during the project to support reporting requirements.
- Research and evidence generation planning

Onboarding Support

my mhealth shall provide training, within the defined period of time, and cost, defined by your procured package.

Onboarding support *may* consist of:

- eLearning Training Modules.
- Account hierarchy setup.
- Working with the customer to understand goal setting within the platform.
- Working with the Customer to understand the current patient pathways and to consider how to develop new integrative pathways, utilising the service.
- Highlighting and exploring the eLearning modules.
- Information Governance support for sign-off.
- All disease-specific applications have a 'how to use' and 'customer support' element integrated, and a bespoke eLearning platform is available for additional support.
- User support is provided via email and ticketing during UK business hours (Monday to Friday). Telephone support is available during office hours. Out-of-hours contact is available for incident notification only.
- Office Hours: call +44 1202 299 583 or email support@mymhealth.com Out of Office Hours: email support@mymhealth.com

Digital Capabilities



Interoperability is supported through secure, documented APIs. Services are deployed behind an API gateway and documented using OpenAPI. APIs enable controlled data exchange and integration where contractually agreed, including support for regional dashboards and service evaluation using anonymised, aggregated data. Authentication and authorisation are managed using industry-standard mechanisms. APIs do not permit modification of core service configuration or regulated clinical functionality, which is managed through the service interface. Integration with NHS services or third-party systems is provided only where contractually agreed and via approved intermediaries.

Pricing Structure

The prices may vary based on the packages that are procured aligned to local needs of clinical and commissioning teams. We can provide you with a variation of bespoke costs relating to your requirements.

Ordering and Invoicing Process

Customers are allocated a designated a point of contact to guide you through the procurement process. Service proposals and subsequent information will be provided to you, along with a purchase order, aligned to customer requirements, an invoice, and a contract for completeness.

Termination

Is subject to the termination clauses agreed in each contract agreement.

Technical Requirements

Supported Web Browser Versions: The platform supports the latest version (N) and the two previous versions (N-2) of major web browsers, unless otherwise indicated. For security and performance reasons, we recommend using the most recent versions.

Safari: WebRTC support begins with Safari version 11.

Edge: Only Chromium-based Edge is supported; legacy Edge is not supported.



	Chrome	Firefox	Safari*	Edge**
Android	✓	✓		
iOS	✓	✓	✓	
Linux	✓	✓		
macOS	✓	✓	✓	
Windows	✓	✓		✓

Supported mobile device requirements: We support both **iOS** and **Android** devices that meet the following requirements:

iOS Devices

- Must have a screen size of 4.7 inches or larger(e.g., iPhone SE (2nd generation) and newer)
- Must still receive security updates from Apple
- Supported iPads include models that are actively maintained by Apple, such as iPad (6th gen) and newer

Android Devices

- Must have a screen size of 4.7 inches or larger
- Must have a minimum resolution of 720 × 1280 pixels (HD)
- Must be running a version of Android that is still receiving security updates from the device manufacturer

Devices that are no longer supported by Apple or Android manufacturers, or that have smaller screens or lower resolutions, may not display content properly and are not eligible for support.

Browser Plug-Ins:

No additional software, such as Flash or Java, is required to use the my mhealth platform.

Technical Requirements to Implement the Service:

For Patients / Users:

- Download the my mhealth app from the Apple App Store or Google Play Store, or
- Access via a supported web browser
- Two-factor authentication (2FA) is enforced for all patient accounts to ensure secure access and protect personal health information

For Clinical Team Members: Network administrators may need to allow access to:

- the **mymhealth.com** domain
- the Vimeo content delivery network, which hosts video educational resources used by the platform
- Two-factor authentication (2FA) is mandatory for all clinical team accounts, ensuring secure access to patient and service data



These measures ensure both patients and clinical teams access the platform securely, in compliance with GDPR, NHS security standards, and medical device requirements.

Network and System Security

Data in Transit:

Data in transit is secured by restricting connections to TLS v1.2 only, utilising updated and secure ciphers, such as AES 256 where possible. Insecure protocols, ciphers, and configurations-such as RC4, SSL3, non-perfect forward secrecy, and client renegotiation-are disabled to ensure robust security. The specific ciphers used for data in transit include:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Operational Work Involving Security:

- **Systems Security Patching:** Regular updates and patches are applied to ensure system security and protect against vulnerabilities.
- **Internal and External Security Audits:** Comprehensive security audits are conducted both internally and externally to assess and enhance the security posture.
- **Software Quality Assurance:** A rigorous software quality assurance process is in place, including application security updates as an integral part of the software development lifecycle.
- **Network Configuration Policies:** Policies governing network configuration are established to ensure secure and efficient operation.
- **Security Advisory Reviews:** Regular reviews are conducted, covering the full stack of software components, to address and mitigate potential security risks.
- **Staff Security Training:** All staff receive ongoing training on the latest security practices to maintain and improve security across all operations.

Physical Security Hosting infrastructure:

my mhealth Limited is not authorised to disclose detailed information regarding the hosting infrastructure. For compliance documents, please refer to the AWS Artefact service, accessible under a Non-Disclosure Agreement (NDA).

my mhealth operates a fully remote working environment, utilising cloud-based hosting software, and therefore does not have any physical premises. All employees receive annual cybersecurity and information governance training, at a minimum, and are governed by a robust set of policies and procedures, including, but not limited to, a clear desk policy and an acceptable use policy.

Application Security:

Content Security Policy (CSP) and Secure Cookies:

CSP, secure cookies, and HTTP-only cookies are enforced in all HTTP communications to ensure data integrity and security.

Authentication Cookies:

Authentication cookies are both encrypted and salted for enhanced security.

Password Security:

Passwords are hashed using PBKDF2, providing robust protection against brute-force attacks.

Data Filtering:

Incoming data is filtered using OWASP sanitisation techniques at the point of reception, ensuring that only safe



data is processed.

Database Security:

HTML and application code are strictly prohibited as content in the database to prevent code injection attacks.

Browser Security:

Data caching is disabled in web browsers to protect sensitive information from being stored locally.

Token Expiry:

Tokens sent to users are designed to expire within 3 hours or after a single use, whichever comes first, to minimise the risk of token misuse.

Operational Security in Development:

Operational security includes the separation of testing and production environments, ensuring that no secrets are stored in source control.

IT Change Management:

A documented IT Change Management procedure is in place for information assets, covering development, functional and non-functional testing processes.

Security Code Reviews:

Security code reviews are routinely conducted, and all code changes are logged in a version control system for traceability.

Malicious Code Protection:

A layered approach is utilised for virus and malicious code protection, safeguarding against multiple attack vectors.

Data-Level Security:

The system employs OWASP components to filter all incoming and outgoing data, protecting against malicious code.

Deployment Security:

At the deployment level, projects are regularly reviewed using Dependency Track and AWS Elastic Container Registry (ECR) image scanning results, with necessary fixes applied promptly.

Certifications and Penetration Testing:

my mhealth maintains its Cyber Essentials Plus certification through annual assessments. Additionally, the platform undergoes an annual external accredited Penetration Test, followed by quarterly vulnerability scans, with all identified issues resolved regardless of severity.

Service Levels

Office Hours: means 08:00 until 17:00 UTC from Monday to Friday except UK Bank Holidays.

Recovery Point Objective: means the maximum targeted period in which data might be lost from the Service due to a major incident.

Recovery Time Objective: means the targeted duration of time and a service level within which the Service will be restored after a disaster or disruption.

1. Network Service

1.1. We will use reasonable commercial efforts to provide a network service availability with a monthly availability percentage of at least 99.9%.

1.2. Unavailability of this Service means when any of the running application services have no external connectivity.



2. Storage Service

- 2.1. We will use reasonable commercial efforts to provide availability of storage service at a monthly availability percentage of at least 99.9%.
- 2.2. Unavailability of this Service means when all of attached storage volumes perform zero read-write IO, with pending IO in the queue.
- 2.3. Disaster Recovery provisions will match the Recovery Time Objective and Recovery Point Objective of this SLA. These include redundant database nodes and both local and off-site data backups.

3. IT Service Support

- 3.1. We will monitor the Service 24 hours per day, 7 days per week.
- 3.2. A team of IT developers/operators will be available during Office Hours to support the Customer and Providers.
- 3.3. Our IT support contacts are: Office Hours: call +44 1202 299 583.

4. Incident reporting and planned maintenance

- 4.1. We will notify you of any incident affecting the Service, including Service unavailability, functionality disruption, data loss or systems hacking.
- 4.2. Although the Service is designed for 24x7 availability, we will inform you at least 24 hours before any planned maintenance activities that potentially or effectively disrupt the Service.
- 4.3. Notification will be made to an individual or department notified by you to us within 48 hours of an incident occurring. You are responsible for keeping us updated on the designated contact. Please write to support@mymhealth.com

5. Service Recovery

- 5.1. Upon incident notification by you or an automated monitoring tool, the Recovery Time Objective will be:
 - a) Two hours for a notification during Office Hours and
 - b) Eight hours during Out-of-Office Hours.
- 5.2. The Recovery Point Objective will be 24 hours or less.

6. SLA Exclusions

- 6.1. This SLA does not apply to availability, quality, performance, correctness or any other issue in relation to the Service in case of:
 - a) Events that are not directly under our reasonable control, including Internet access to our service and misconfigurations in User's devices
 - b) Events resulting from actions or inactions of you or any third party
 - c) Suspension or termination of the Service.

Data Management, Access, and Security

This section outlines how my mhealth Limited handles, processes, stores, and protects data collected through the my mhealth platform, including modules such as myCOPD, myHeart, myAsthma, and myDiabetes. It covers



patient and clinical data, system access, security measures, and hosting environment controls to ensure compliance with UK GDPR, medical device regulations, and information governance standards.

Data Types and Sources

From Patients (Sensitive and Special Category Health Data):

We collect information necessary to support self-management and service delivery, including:

- Personal identifiers: name, NHS number, date of birth, sex, contact details (address, email, phone).
- Health data: symptoms, medication adherence, disease metrics.
- Location data: GPS or postcode, which users can disable.
- System and usage data: login and device information, and video usage analytics for research and service improvement purposes.

Personal Identifiable Data (PID):

Contact details of the patient's clinician, next of kin (if provided), and GP to enable appropriate service support, communication, and continuity of care.

From Clinical Team Members:

Professional information including name, role, email, phone number, and organisation/team.

Additional Notes:

The service does **not** process criminal data.

No patient profiling is undertaken.

All data collection aligns with lawful processing principles under UK GDPR.

Service Utilisation and Data Processing

The platform is a self-management tool, with functionality tailored to patients' conditions and treatment plans. Data processing scales with patient activity. Contractual arrangements and platform controls ensure all data is processed within AWS London regions, maintaining data residency and compliance.

Use of NHS PDS Lookup for Patient Identity Matching

my mhealth uses the NHS Personal Demographics Service (PDS) to verify the identity of users and ensure records are accurately matched to the correct patient. Only the minimum personal data required for the lookup, such as name, date of birth, GP practice and NHS number is used. No additional PDS data is stored within my mhealth beyond what is necessary for verification. Access to the PDS is authorised, audited, and controlled to prevent unauthorised use. The purpose is limited to identity validation and maintaining accurate patient records. The lawful basis for this processing aligns with obligations to provide safe and reliable digital health services.

Access to Data

- **Patients:** Access their own personal and health data.
- **Clinical Team Members:** Access data only for patients under their direct care.
- **Clinical Managers / Admin Accounts:** Access is restricted to administrative setup; no clinical decision-making authority is granted.

Access is granted strictly on a need-to-know basis, with all staff and contractors bound by confidentiality obligations. Only the minimum necessary data is accessed to deliver the service.

Data backup, restore and disaster recovery

Data is stored exclusively within AWS London regions across multiple availability zones, with encryption applied both in transit and at rest using AES-256. Remote access is monitored on a daily basis, and compliance is maintained with ISO 27001, DSPT, and DCB 0129 standards.



Each AZ (London) has its own power infrastructure and is connected with a fast, private fibre-optic network. Data is not stored outside of the UK boundaries.

Data transferred to AWS (Amazon Web Services) is encrypted in transit and at rest and AWS have a series of recognised international standards such as ISO 27001. They can be contacted on; Amazon UK Services Ltd. Patriot Court, 1-9 The Grove, Slough, SL1 1QP, United Kingdom Tel. 0800 496 1081

my mhealth has a fully implemented, tried, and tested disaster recovery plan:

- To minimise the businesses' vulnerability to disaster
- To establish and raise awareness of the procedures and the necessary resources to reduce the impact to the business and consequence of any disaster
- To enable the right decisions to be made, and efficiently, at the time of crisis
- To limit the impact to our clients in the event of a disaster

Certifications/Aligned

Accreditation and Certifications

- Cyber Essentials / Cyber Essentials Plus [Registry Link](#)
- Qismet [Accreditation Register](#)
- Orcha [App Finder](#)
- DTAC
- DSPT [Link](#)
- DCB0129

Aligned with

- ISO 13485:2016 Medical devices — Quality management systems
- ISO 27001:2013 Information Security Management
- IEC 62366-1:2015 Usability Engineering for Medical Devices
- IEC 62304:2006/AMD 1:2015 Medical Device Software Lifecycle Processes
- BS EN ISO 15223-1:2021 Medical Device Symbols
- GCP (Good Clinical Practice)

NICE Early Value Assessments(EVAs)

- NICE EVA for Digital Pulmonary Rehabilitation myCOPD <https://www.nice.org.uk/guidance/htg718>
- NICE EVA for Digital Self Management myCOPD <https://www.nice.org.uk/guidance/htg736>
- NICE EVA for Digital Cardiac Rehabilitation myHeart <https://www.nice.org.uk/guidance/htg764>
- NICE EVA draft for Digital Self Management myAsthma <https://www.nice.org.uk/guidance/indevelopment/gid-hte10063>

Classification

CONFIDENTIAL Available only to specified and relevant members, with appropriate authorisation.



Template Copyright openregulatory.com. See [templatelicense](https://templatelicense.com).

Please don't remove this notice even if you've modified contents of this template.

Template: SOP Template (Heading) (v2) - outdated

Review & Approval

Activity	Date	Name (Role)
Created (v2)	2026-01-15 14:04:38	Nadine Milligan
Review approved	2026-01-28 08:26:25	Carre King (Compliance)
Review approved	2026-01-28 08:30:08	Jane Stokes (Customer Success)
Review approved	2026-01-28 08:49:43	Ian Thompson (Commercial)
Review approved	2026-01-28 14:09:18	Thomas van Lindholm (Chief Technology Officer)
Review approved	2026-01-29 09:55:43	Nadine Milligan (Operations Manager)
Review approved	2026-01-29 09:55:54	Nadine Milligan (DPO)

Description of Changes:

Jane's comments have now been addressed.

Approved Review by Carre King as Compliance:

No comment provided.

Approved Review by Jane Stokes as Customer Success:

No comment provided.

Approved Review by Ian Thompson as Commercial:

No comment provided.

Approved Review by Thomas van Lindholm as Chief Technology Officer:

No comment provided.



Approved Review by Nadine Milligan as Operations Manager:

No comment provided.

Approved Review by Nadine Milligan as DPO:

No comment provided.