Scope and Use of this DPIA

This Data Protection Impact Assessment (DPIA) is provided as a guidance resource and reflects the data protection and privacy controls implemented by my mhealth Limited for the platform. It is not a substitute for local risk assessments.

All participating sites, clinical teams, or partner organisations are responsible for conducting their own information governance and risk assessments in accordance with local policies, procedures, and regulatory requirements prior to accessing or using the platform.

This DPIA should be used to inform local processes, support compliance, and guide discussions around data protection, but it does not relieve any site or user of their obligations under UK GDPR, NHS policies, or other applicable legislation.

Name and purpose of the Project

Deployment of the my mhealth Application
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.

Supplier Information

Company Name: my mhealth Limited
Registered Address: 41 Lothbury, London, EC2R 7HF
Company Registration Number: 07881370
NHS Organisation Code: 8JH30
DUNS Number: 218147428
Information Commissioner's Office (ICO) Registration ICO Registration
Registration Number: ZA151364

Regulatory Compliance

my mhealth Limited is fully compliant with the following regulatory requirements:

- **Medical Devices Regulations 2002 (SI 2002 No 618, as amended)**
- **FDA 21 CFR Part 11**
- **FDA 21 CFR Part 820**

Advisory Standards Compliance
my mhealth Limited adheres to recognised advisory standards, including:

- **DCB 0129** Clinical Risk Management for Health IT
- **DTAC** Digital Technology Assessment Criteria

Designated Standards and Other Applicable Regulations
my mhealth Limited complies with UK designated standards and international standards relevant to medical devices and information security:

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

The **Declaration of Conformity** for my mhealth Limited is available upon request.

Policies and Clinical Risk Management
Robust governance underpins all clinical and technical processes. Policies cover physical access control, secure mobile working, acceptable use of devices, and the secure delivery of sensitive credentials.

Clinical risk and safety (DCB 0129) is overseen by the company's Clinical Safety Officer, ensuring all clinical content and platform functionality adhere to NICE or other nationally recognised guidelines. Data protection is embedded throughout, with controlled access, audit trails, and monitoring to maintain confidentiality, integrity, and availability. All changes to the

platform, including software updates, clinical content, and data handling processes, follow a formal change management procedure with risk assessment, review, and approval to ensure safety, compliance, and data quality.

Incident management and reporting mechanisms provide full traceability and accountability.

Detailed clinical safety and risk management information is available separately on request.

Supplier Accreditations, Compliance, and Security Measures

Accreditations and Certifications
my mhealth holds recognised certifications and accreditations, including:
Cyber Essentials / Cyber Essentials Plus Registry
Qismet Accreditation Register
Orcha App Finder

Data Security Compliance
my mhealth is fully compliant with the NHS Data Security and Protection Toolkit: DSP Toolkit.

Access and Authentication
The platform supports single sign-on via NHS login. Patients may also log in using a username and password with two-factor authentication. Access to patient and clinical data is role-based, controlled, and monitored in line with GDPR and medical device requirements.

Commercial Frameworks
my mhealth is listed on recognised commercial frameworks, including DPS Spark, The London Procurement Partnership, HSSF, and G-Cloud.

Employee and Contractor Screening
All employees, both existing and new, undergo DBS checks at a level appropriate to their role. Selected contractors are screened as required and sign agreements to comply with legal and regulatory obligations, including data protection, confidentiality, and intellectual property.

Training and Awareness
All staff complete mandatory data protection, information security, and medical device compliance training during induction, with annual refresher training. Training covers GDPR, secure handling of sensitive health data, breach reporting, secure software use, and clinical risk awareness relevant to medical devices. Compliance with training requirements is formally monitored.

Customer Support
my mhealth provides setup and ongoing support for both patients and clinical services. Support is delivered through dedicated teams to ensure timely assistance, guidance, and troubleshooting for all users, including clinical and operational stakeholders.

Business Continuity and Disaster Recovery
A fully documented disaster recovery and business continuity plan is in place, with quarterly testing conducted via penetration testing to ensure resilience and readiness in the event of service disruption. Critical systems, data, and recovery procedures are reviewed and audited to maintain medical device compliance.

Information Security and Data Breach Management
my mhealth maintains comprehensive information security and data breach policies. Any data breach is promptly reported to the designated customer contact, the Data Protection Officer (DPO), and, where applicable, to the Information Commissioner's Office (ICO).

All breaches are formally recorded, monitored, and analysed to ensure accountability, continuous improvement, and regulatory compliance.

Product Information

Category of Product: Software as a Service (SaaS)
DTAC Assessed: Yes
MHRA Registration: The my mhealth platform is registered with the Medicines and Healthcare products Regulatory Authority (MHRA) as a Class I medical device.
UKCA Marking: The platform bears a UKCA marking for quality and safety, which can be viewed on the supplier website: www.mymhealth.com.
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.

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
- **Validated condition-specific assessments:** At timed intervals that generates personalised advice and automates conventional review processes - saving time
- **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.
- **NICE EVA Published April 2024:** Recommends myCOPD as a Digital technology to deliver Pulmonary Rehabilitation for adults with COPD

<u>Network and System Security</u>

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.

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 Access, Logging, and Transparency

- **Logging:** All system access is logged, including entry, duration, and activity.
- **Backups:** Data is backed up securely using AES-256 encryption via AWS.
- **Transparency:** Users are informed about data collection and sharing at onboarding and must accept the Privacy Policy and Terms and Conditions.

Data Storage and Security

- Data is stored exclusively within AWS London regions across multiple availability zones.
- Encryption is applied in transit and at rest using AES-256.
- Remote access is monitored daily.
- Compliance is maintained with ISO 27001, DSPT, and DCB 0129 standards.
- Data sharing is governed by contracts with customers, which include data governance clauses and Service Level Agreements (SLA).
- Users may request corrections or deletion of their data in line with GDPR. Deleting the app from a device does not remove data stored on the platform.

Hosting Environment Security

The my mhealth platform is hosted exclusively within AWS London regions. Security controls include:

- **Encryption:** All data encrypted in transit and at rest (AES-256).
- **Access Controls:** Role-based access and multi-factor authentication are enforced.
- **Monitoring and Threat Detection:** AWS GuardDuty monitors for potential threats, including malware, unauthorised activity, and suspicious behaviour.
- **Anti-Virus / Malware Protection:** GuardDuty forms part of the platform's active anti-virus and intrusion detection strategy.
- **Backup and Disaster Recovery:** Data is securely backed up across multiple availability zones, with quarterly disaster recovery and penetration testing conducted to ensure resilience.

These measures ensure the hosting environment is actively monitored and protected against cyber threats in line with ISO 27001, DSPT, and DCB 0129 standards.

AWS Contact Information

Amazon UK Services Ltd.
Patriot Court, 1-9 The Grove, Slough, SL1 1QP, United Kingdom
Tel: 0800 496 1081

Lawful basis for processing

For more detailed information on how my mhealth handles personal data, please refer to the my mhealth Privacy Policy. The following outlines the purposes of processing and the lawful bases relied upon.

Account creation and management

To create, register, and manage user accounts for the app(s) and service(s), my mhealth acts as a Joint Controller with the user's healthcare team. The lawful basis is performance of a contract, with healthcare purposes applying where special category data is processed.

Service updates and notifications

To keep users informed of changes, modifications, or updates to the app(s) and service(s), my mhealth relies on legitimate interests.

Issue resolution and safety
For addressing and resolving issues that may affect use of the app(s) and services, my mhealth processes data under legitimate interests to maintain safety, security, and service continuity.
Quality improvement and testing
Troubleshooting, data quality checks, functional testing, security testing, and statistical analyses are carried out under legitimate interests to assess and improve the quality and reliability of services.
Record keeping
To maintain accurate and up-to-date records, my mhealth acts as a Joint Controller with the user's healthcare team. Processing is based on legitimate interests to ensure provision of relevant content and continuity of care.
Legal and regulatory obligations
Processing undertaken to meet legal, regulatory, and risk management obligations, including reporting and disclosure requirements, is based on legal obligations.
Fraud prevention
To safeguard the integrity of services and protect users, my mhealth processes data under legitimate interests for fraud prevention.
Protecting the rights of third parties
Where necessary to protect the rights of third parties, my mhealth processes data under legal obligations and legitimate interests, including cooperation with law enforcement or regulatory bodies.
Enforcing legal rights
For the establishment, exercise, or defence of legal claims, processing may occur under legal obligations and for legal claims.
Data anonymisation and research
Anonymisation is carried out to ensure data cannot identify individuals. Anonymised data may be shared with researchers to support scientific studies, guidelines, and treatment development. This is based on legitimate interests.
Information sharing with healthcare teams
When sharing information with healthcare teams via the app(s), my mhealth acts as a Joint Controller with the healthcare team. The lawful basis is performance of a contract and healthcare purposes for special category data, aimed at supporting the management of medical conditions.
Contacting users about clinical studies
Where users are contacted about clinical studies or research trials relevant to their condition, this is carried out on the basis of consent and, where applicable, explicit consent for special category data.
Service evaluations and trials
Contact regarding service evaluations, studies, or trials run by my mhealth is based on consent and, where appropriate, legitimate interests.
Educational progress monitoring
Reviewing a user's progress through educational materials and courses is necessary for service provision and is based on contract performance. Legitimate interests may also apply to improve user experience and service delivery.
Understanding service use
Analysing how users interact with the app(s) and website, including most visited areas, is carried out under legitimate interests. This supports effective management of medical conditions and continuous service development.

Compliance with disclosure requirements
Where disclosure to government, regulatory, or law enforcement authorities is required, my mhealth relies on legal obligations. Where feasible, or where it does not hinder crime prevention or detection, individuals are notified prior to responding to such requests.

Data Relationships and Roles

Data Controller and Joint Controller Relationships
This section outlines the legal relationships and responsibilities regarding the processing of personal and health data within the my mhealth platform. The explicit details, including legal bases for processing, are set out in the my mhealth Privacy Policy. Here, we provide an overview and rationale for the key data processing relationships:

Relationship Between Healthcare Professionals and Users

Healthcare Professionals as Data Controllers
Healthcare professionals entering data or communications into the platform act as Data Controllers for that information. my mhealth Limited (MMH) acts as a Data Processor under the lawful basis provided by the healthcare professional. This is in accordance with:

- **Article 6(1)(e) GDPR** – performance of a task carried out in the public interest, and
- **Article 9(2)(h) GDPR** – processing of special category data for healthcare purposes.

MMH as Data Controller
For certain data entered by healthcare professionals on behalf of patients (for example, clinical measurements such as blood pressure readings), MMH assumes the role of Data Controller to deliver the agreed service. This ensures compliance with:

- **Article 5(1)(b) GDPR** – purpose limitation, and
- **Article 5(1)(c) GDPR** – data minimisation.

Joint Controllers
Where healthcare professionals access patient data within their clinician accounts, they act as Joint Controllers with MMH for that shared data. This arrangement complies with Article 26 GDPR, and responsibilities for processing, security, and transparency are clearly defined and communicated to users.

Rationale for Joint Controller Approach
This structured joint controller framework ensures:

- **Clear delineation of responsibilities** between MMH, healthcare professionals, and procuring organisations.
- **Legal clarity** for GDPR compliance and special category data handling.
- **Transparency for patients** regarding who controls, accesses, and processes their data.
- **Risk mitigation** by defining accountability for data security, retention, and lawful processing.

Relationship Between the Procuring Organisation and MMH

Procuring Organisation as Data Controller
The procuring organisation, which provides access to the clinical dashboard, acts as Data Controller for Clinical Team Members' data within the platform. MMH acts as Data Processor, with responsibilities defined under Article 28(1) GDPR and contractual obligations under Article 28(3) GDPR.

Lawful Basis for Processing
Data is processed under the procuring organisation's lawful bases:

- **Article 6(1)(e) GDPR** – performance of a public interest task, and
- **Article 9(2)(h) GDPR** – special category data for healthcare purposes.

Contract Expiry
Upon contract expiry, access to the clinical dashboard is revoked. Patients continue to have access to self-management tools, with MMH retaining its role as Data Controller for ongoing patient-entered data. Data is managed in accordance with the storage limitation principle (Article 5(1)(e) GDPR).

Relationship Between Patients and MMH

Direct Relationship
A direct relationship is established when patients accept the Terms and Conditions and Privacy Policy during onboarding.
MMH as Data Controller

- MMH is the Data Controller for all patient-entered data.
- Clinical staff may initially act as Data Controllers when entering data on behalf of patients, with MMH operating as Data Processor until the user takes ownership of their account.
- Once patients are onboarded, MMH becomes the sole Data Controller for patient-entered information.

Lawful Bases for Processing

- **Article 6(1)(b) GDPR** – performance of a contract.
- **Article 9(2)(h) GDPR** – processing of special category data for healthcare purposes.

Legitimate Interests
For certain platform functions (such as service improvement or feature updates), MMH may process data under Article 6(1)(f) GDPR (legitimate interests), following appropriate balancing tests to ensure fairness to users.
Transparency and Compliance
MMH ensures compliance with:

- Articles 13 and 25 GDPR – transparency, data protection by design and by default, and user information.
- Processing is limited strictly to what is necessary for the services provided.

- Age restrictions, such as for the myAsthma module (available to individuals aged 13+), are implemented and detailed in the Privacy Policy.

Data Retention

We retain personal information only for as long as necessary to fulfil the purpose for which it was originally collected, including any related legal and regulatory obligations.

Our data retention periods are determined by our business needs and align with established NHS guidelines for managing long-term illness records. These periods are regularly reviewed to ensure that data is not retained longer than necessary. Personal information will be retained for up to 20 years from the last interaction with the platform, or until a request for deletion is made, in accordance with NHS record-keeping requirements. In the event of a user's death, their data will be deleted after 10 years, in line with medical guidelines.

After 20 years, data will be anonymised in accordance with Article 5(e) of the UK General Data Protection Regulation (GDPR) and used solely for clinical research or statistical studies. Anonymised data will not be re-identifiable, and our system includes scripts to automatically anonymise and archive such data. All identifiable information is removed from the my mhealth platform once the retention period ends. Anonymised data is stored within the my mhealth insights platform.

Users may opt out of communications and request deletion of their personal data in accordance with GDPR. Such requests will be handled by our support team, and users will be notified once their request has been completed. Please note that deleting the application from a device does not remove data stored within the platform. Patients can request corrections to their personal data, while clinical team members can make limited edits via a web browser or the my mhealth app, but only for users within their own account structure.

If services are no longer required, or if a contract expires or is terminated, access to the clinical dashboard will be revoked, and data will be retained in line with the my mhealth data retention policy.

General FAQs

How will you provide privacy information to individuals?
Patients are provided with the Terms and Conditions and Privacy Policy, which must be read and accepted to access the service. Any updates to the Privacy Policy are communicated to users. These documents outline what personal data is collected, why it is processed, who has access, retention periods, anonymisation procedures, and individuals' rights under data protection law.
Does the processing achieve your purpose?
Yes. my mhealth processes personal and sensitive data only for clearly defined purposes, with the lawful basis for processing documented for each use.
What information will you give individuals?
Patients are informed about:

- The types of personal data collected, including health information, contact details, and usage data.
- The purposes for which data is collected and used, such as account management, service improvement, and legal obligations.
- How data is processed, including lawful bases under GDPR.

- Who has access to their data and under what circumstances, including clinical teams or researchers.
- Data retention periods and anonymisation processes.
- Their rights under data protection law, such as access, correction, and deletion, and how to exercise them.
- Security measures protecting personal data, including encryption, access controls, and monitoring.

How will you support individuals' rights?
my mhealth supports GDPR rights by providing guidance in the Privacy Policy. Users can access, amend, or request deletion of their data via the app, Customer Support, or the 'My Account' section.
Will reports be generated? If yes, will the information be identifiable or anonymous (will the reports be used for research)?
Reports are generated for service evaluation, contractual monitoring, and platform usage. These are aggregated and anonymised to prevent identification.

- Identifiable data may be used for direct care purposes only with a lawful basis and limited to authorised personnel.
- For HRA-approved research, identifiable data may be used with explicit informed consent and full ethical safeguards. All other reporting remains non-identifiable.

Can users request their data to be removed?
Yes. Users can request data removal in line with GDPR. Requests are processed by our support team, with confirmation once complete. Deleting the app does not automatically remove stored data. Requests can be submitted via the app, Customer Support, or the 'My Account' section.
NHS login terms
Please note that if you access our service using your NHS login details, the identity verification services are managed by NHS England. NHS England is the controller for any personal information you provided to NHS England to get an NHS login account and verify your identity, and uses the personal information provided solely for that single purpose. For this personal information, our role is a "processor" only and we must act under the instructions provided by NHS England (as the "controller") when verifying your identity. To see NHS England's Privacy Notice and Terms and Conditions, please click here.
How will you prevent function creep?
Function creep is prevented through strict contractual agreements and comprehensive training covering the permitted use of each product module.
How do you intend to ensure data quality?
Data quality is maintained through:

- **User updates:** Patients can view and update their own information.
- **Internal controls:** Source control, automated/manual testing, regression checks, and formal change management.
- *Clinical review is optional and not required for the platform to function within its intended use.*

What safeguards are in place for international data transfers?
No international data transfers are conducted.
Does the app send any direct electronic messages, including emails, text messages, or reminders?
The app sends automated **in-app reminders and notifications** (e.g., medication prompts), which users can disable. Emails and text messages may also be sent to consented users or where there is a legitimate interest, such as newsletters or feature updates. All messages comply with legislation, include unsubscribe options, and do not support two-way messaging.
What will happen to the information if the organisation/service ceases?
Patients retain privacy controls to manage data access, including granting or revoking access to NHS clinical teams. Migration procedures are agreed prior to decommissioning infrastructure.
What measures do my mhealth implement to prevent unauthorised access to systems from outside the company?

- **Encryption:** All data is encrypted in transit and at rest.
- **DDoS Protection:** AWS Shield protects against attacks.
- **Content Security:** CSP mitigates XSS attacks; secure, HTTP-only cookies are used.
- **Authentication & 2FA:** Mandatory two-factor authentication for all patients and clinical users; passwords hashed with PBKDF2.
- **Data Filtering & Storage:** OWASP sanitisation prevents injection; HTML/code not stored in the database.
- **Cache & Token Management:** Browser caching disabled; tokens expire after 3 hours or on first use.
- **Password Lockout:** Implemented to prevent brute-force attacks.
- **Monitoring & Alerts:** Prometheus and Grafana monitor in real time; alerts sent to DevOps team; cluster is largely self-healing.
- **Incident Management:** Daily stand-ups review and prioritise incidents.
- **Security Testing:** Regular external penetration testing and vulnerability scanning.

Cloud Service Contingency
Full control of data is maintained.
AWS provides 30 days' notice of contract termination for data transfer.
Agreements ensure secure deletion of data from original storage after successful transfer.
Customer environments are segregated to prevent data leakage.
AWS Managed Services provides 24/7 monitoring and rapid response to vulnerabilities.

Service Level Agreement

Is available via our website

Contacts

Head of Compliance:

- Phone: 01202 299 583
- Email: Compliance@mymhealth.com

Data Protection Officer:

- Phone: 01202 299 583
- Email: DPO@mymhealth.com

Senior Information Risk Owner (SIRO):

- Phone: 01202 299 583
- Email: David.Pettigrew@mymhealth.com