This DPIA (Data Protection Impact Assessment) is provided as a resource only and is not intended to be used to identify your own risks. All sites involved in the project will need to complete their own local information governance processes prior to accessing the platform.

Name of the Project

Deployment of my mhealth application(s)

Describe the purpose or aim(s) of the project

myCOPD, myHeart, myAsthma, and myDiabetes are web-based applications developed by my mhealth Limited. These applications are designed to support patients in self-managing chronic conditions and to enable clinical teams to manage patient populations remotely and at scale throughout the entire care pathway.

Aims:

Enhance Self-Management: The primary aim is to provide licences to patients diagnosed with one or more of the supported chronic conditions (subject to contracted access). This facilitates improved self-care outside of clinical settings through the use of the apps.
Improve Patient Outcomes: By engaging, educating, and empowering patients, my mhealth aims to enhance patient outcomes and reduce healthcare costs.
Enable New Models of Care: The platform supports clinical teams in delivering innovative care models at a population scale, leveraging technology for more effective patient management.
Generate and Utilise Evidence: my mhealth has a proven track record of securing grant funding from sources such as SBRI and Innovate UK. The company has completed trials that provide compelling evidence supporting the platform's efficacy. Research is published on the supplier website.
Real-World Effectiveness: The platform's effectiveness is also supported by real-world data, showing comparable outcomes to standard cardiac and pulmonary rehabilitation offerings. Independent post-market surveillance indicates high user satisfaction, with users finding the platform easy to use and recommending it to others.
Healthcare System Engagement:
my mhealth has achieved market-leading engagement with the NHS, with a growing user base each month, reflecting the platform's effectiveness and relevance in the healthcare system.

Supplier Information

Supplier details

my mhealth Limited

Registered address

Milton Gate
60 Chiswell Street
London
EC1Y 4AG

Registration number

07881370

NHS organisation code

8JH30

DUNS number

218147428

Is the supplier registered with the ICO?

Yes See HERE

Registration number:

ZA151364

Is the supplier compliant with any regulatory standards?

The my mhealth deceleration of conformity is available upon request.

my mhealth Limited is compliant with regulation(s):
Medical Devices Regulations 2002 (SI 2002 No 618, as amended)
FDA 21 CFR Part 11
FDA 21 CFR Part 820

my mhealth Limited is complaint with advisory standard(s):
DCB 0129
DTAC Digital Technology Assessment Criteria

my mhealth Limited adheres to UK designated standards and other applicable regulations:
BS EN ISO 15223-1:2021
GCP (Good Clinical Practice)
IEC 62304: 2006/AMD 1:2015
IEC 62366-1:2015
ISO 27001: 2013
ISO 13485: 2016

Does the Supplier have any accreditations or certifications?

Yes, please see these below:
Cyber Essentials/Cyber Essentials Plus
https://registry.blockmarktech.com/organisations/GBLTD07881370/
Qismet
https://www.qismet.org.uk/accreditation/accreditation-register/
Orcha
https://appfinder.orcha.co.uk/

Is the supplier compliant with the Data Security Protection Toolkit?

Yes
https://www.dsptoolkit.nhs.uk/OrganisationSearch/8JH30

Does the supplier have the ability to provide single login?

Yes, we are enabled via NHS login. All patients can choose to login via a password and username enabled with two factor authentication or via NHS login.

Does the Supplier appear on any commercial Frameworks?

Yes, DPS Spark, The London Procurement partnership, HSSF, GCloud

What screening is carried out on new employees / contractors?

All existing and new employees have updated DBS (Disclosure and Barring Service) checks, at a level relevant to their employment.
Carefully selected contractors also undergo applicable checks and have signed agreements to comply with all relevant obligations under prevailing laws and regulations, including those related to data security, confidentiality, and intellectual property.

Does the supplier conduct mandatory security awareness training with all employees?

Yes, this is delivered upon Induction and annually at minimum

Do my mhealth provide set up and ongoing support?

Yes, my mhealth provides setup and ongoing support. We have a dedicated customer support team, as well as customer success and operations divisions, to ensure our customers receive the assistance they need. The level of support varies depending on the selected package option.

Does the supplier have measures in place to ensure continued trade from suffering a disaster?

my mhealth have an embedded and audit ready disaster recovery plan.

Does the Supplier have information security policies?

Yes

Does the supplier have a data breach policy?

Yes

How will data breaches be reported?

my mhealth Limited will notify the designated contact of any breach. If applicable, the breach will also be reported to the Information Commissioner's Office (ICO).

Does the supplier keep records of all data breaches?

Yes

Product Information

Category of product

Software as a service (SaaS)

DTAC Assessed?

Yes

Registered with the MHRA (Medicine and Healthcare Research Authority) as a medical device?

Yes Class 1 See HERE

Does the platform bear a UKCA marking for quality and safety?

Yes, this can be viewed on the supplier website www.mymhealth.com

Supported web browser versions?

We support the most recent (N) and the two previous (N-2) versions of these browsers unless otherwise indicated. For security reasons we recommend using the latest versions available

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

* WebRTC support in Safari started with Safari version 11
** We support Chromium-based Edge only. Legacy Edge isn't supported.

Are any browser plug-ins required?

No additional software is required, such as Flash or Java

Are there any technical requirements to implement the service?

For users:
a) Download the my mhealth app from Play Store or Apple Store
b) Or use their preferred web browser.

For Clinical team members:
Clinical team members may need their network administrator to allow access to:
a) the mymhealth.com domain on the Internet.
b) the Vimeo content delivery network on the Internet. This holds video educational resources utilised by the app

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

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

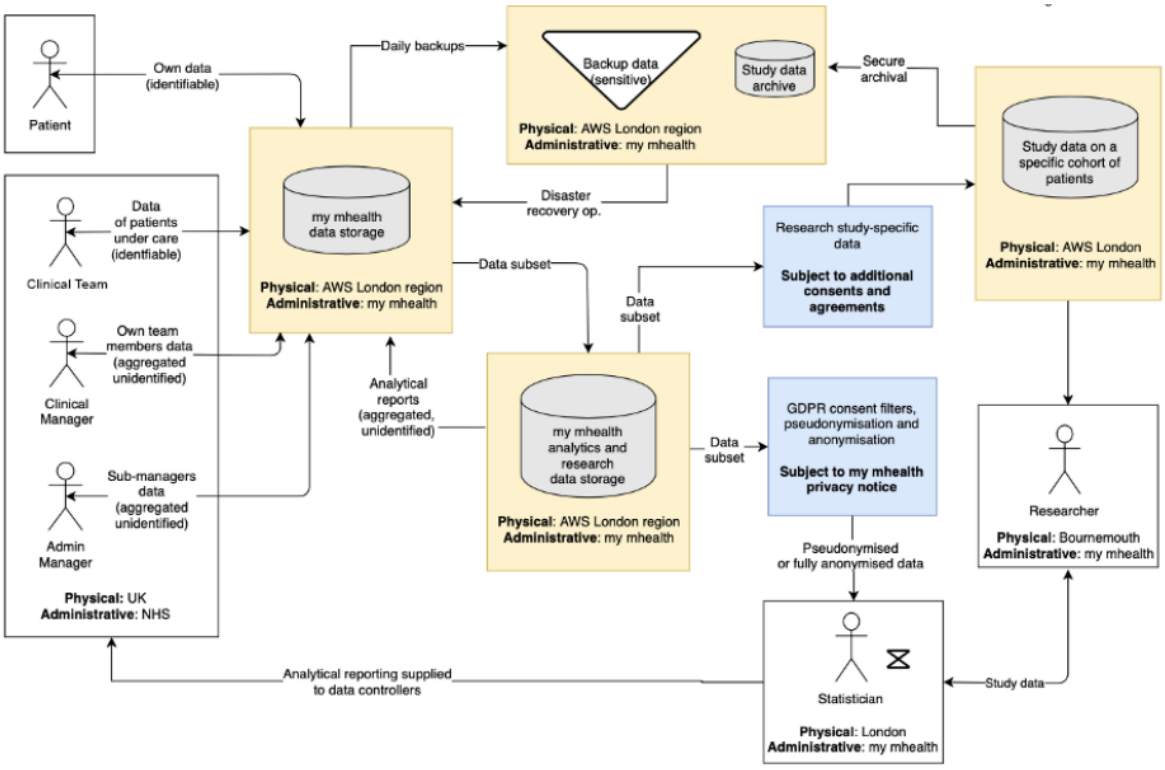
set of policies and procedures, including, but not limited to, a clear desk policy and an acceptable use policy.

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.

Data Collection, Processing and Storage

Data collected through the service is to support patients to self-manage their condition(s), enabling clinical teams to manage patient populations at scale for specific long-term diseases. The data flow through the service is demonstrated in the following;



Security and Quality Management Systems:
my mhealth has embedded management systems to ensure the security and quality of its systems and the data within. All data collected, processed, and stored is protected using AES-256 encryption both in transit and at rest. Data transfers occur exclusively via network-only TLS 1.2, including transmissions from the my mhealth interface to backup and system hosts (AWS). Remote access to infrastructure holding patient data is monitored daily, and the company complies with the requirements of the Data Security and Protection Toolkit (DSPT) and the DCB 0129.

Policies and Clinical Risk Management:
Our management systems include policies for physical access control, mobile work, acceptable use of devices, and the delivery of sensitive access details. Clinical Risk Safety (DCB 0129) is managed by the company's Clinical safety officer. All clinical guidance and references within the platform adhere to NICE (National Institute for Health and Care Excellence) or other nationally accepted guidelines. Detailed information on Clinical Safety is available separately upon request.

Patient Data Collection and Security:
Patient data, including identifiable and special category data, is collected directly through individual accounts controlled by user-chosen login credentials or NHS Login. Two Factor Authentication is employed with an email address and password, in alignment with my mhealth's password policy. Clinical team members can also input data such as observations and medication changes following patient appointments.

Clinical Team Data Collection and Security:
Clinical team data is collected through top-level and clinical manager accounts, with individual accounts accessible via email address and password, also with Two Factor Authentication. This data is used to generate aggregated anonymised performance reports for clinical teams, as stipulated in contractual agreements. my mhealth does not use individual clinical team data beyond this purpose.

Data Storage and AWS Infrastructure:
Data is stored exclusively within Amazon Web Services (AWS) London regions. The cloud service operates with a database cluster across three separate locations to minimise downtime. Each region is fully partitioned with availability zones (AZs) for enhanced isolation and high availability. Each AZ has its own power infrastructure and is linked via a private, high-speed fibre-optic network. AWS London comprises a cluster of Tier-4 connected data centres. Data is not stored outside the UK and is encrypted in transit and at rest. AWS complies with recognised international standards, including ISO 27001.

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

We Use the Collected Data To:

Provide a Service:

- To grant access to our service and manage user accounts.
- To inform users about changes, modifications, and updates to the service.
- To review, investigate, and address any issues affecting the use of our service.

Exercise Legitimate Interest:

- To review and assess the quality of our service and implement improvements.
- To provide responsive support to both patients and healthcare professionals, either through the app(s) or our customer support team.
- For internal operations, including troubleshooting, data quality checks, functional testing, security, audit, and statistical analysis. This is done using anonymised data only.

Consent to Research Opportunities:

- my mhealth participates in research and may contact users about research opportunities. Users are asked to consent to being contacted or receiving information about research via an opt-in/out preference setting.
- Users who opt in agree to be contacted directly or via the app about research opportunities. Users who opt out will not be contacted, and their decision will be noted. Opting out does not affect access to or functionality of the app.

Respond to Obligatory Requirements:

- To comply with regulatory requirements or legal requests.
- Information may be shared with:
    - **Data Backup Services (AWS):** To back up information entered into user accounts. AWS may access identifiable data only if required by law; otherwise, they have no visibility into this data, controlled via contractual agreements.
    - **Push Notification Providers:** To send medication reminders and updates from healthcare teams, helping patients adhere to medication plans and facilitating clinician communication via in-app functions.
    - **Healthcare & Research Teams:** To evaluate and improve the service, and to assist in studies, evaluations, and medical research with relevant authorities' approval. Explicit consent is obtained to contact users for these purposes via our privacy policy and opt-in/out settings.
    - **SMS Messaging Services:** To communicate information relevant to users' conditions, where healthcare teams have prior approval for these systems.

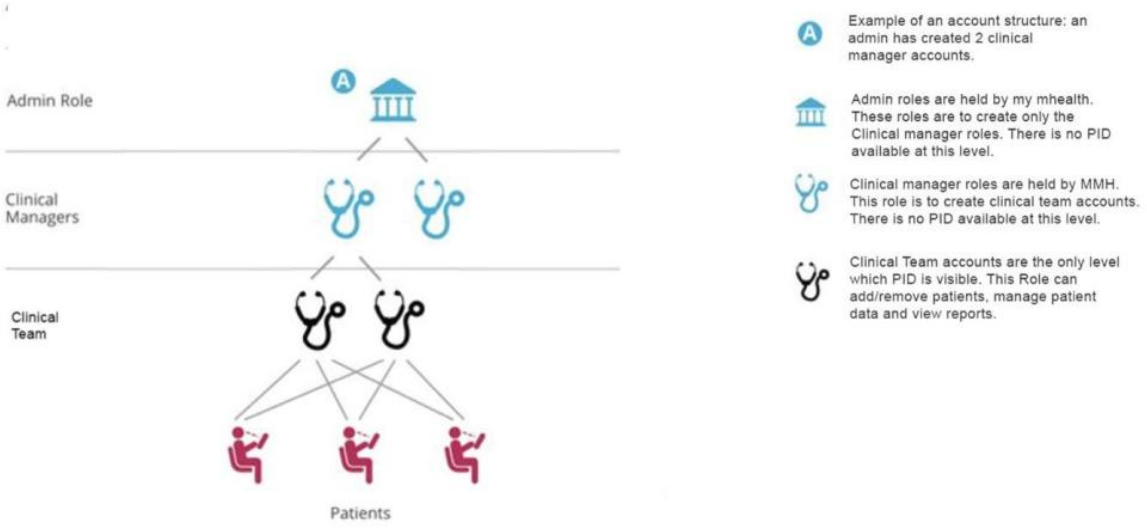
Data Management and Privacy:

- Data sharing is governed by a contract with customers that includes data governance clauses and a Service Level Agreement (SLA).

Sharing of user data is managed according to our privacy policy, available at www.mymhealth.com/privacy.

Data Collected

- **From Patients (Sensitive and Special Category Health Data):**
    - Basic contact details, name, address, symptoms, medication adherence, location (GPS/postcode; can be disabled by the user), disease details and metrics, research analytics data (including video usage), login details, and device information (for service evaluation and improvement).
- **Personal Identifiable Data (PID):**
    - Contact details of the patient’s clinician, next of kin, and GP. Special category data includes health-related information entered by the patient.
- **From Clinical Team Members (Corporate Data):**
    - Name, role, email address, telephone number, and organisation or team name. The service does not collect or process criminal data and does not involve patient profiling.



Service Utilisation and Data Processing:
The service is designed for patients to use as a self-management tool, with usage frequency tailored to their condition, medication, and self-management plan requirements. Data processing is continuous and scales with the number of patients onboarded to the platform. Contractual arrangements and setup controls ensure data is processed within the AWS London regions.

Access to Personal and Special Category Data:

- **Patients:** Have access to their own data.
- **Clinical Team Members:** Can access data for patients under their direct care.
- **Clinical Managers and Top-Level Accounts:** Managed by our Operations division to support administrative setup for clinical teams and reduce time burdens.

Access to data is restricted to named, designated full-time employees who are bound by confidentiality clauses and operate on a need-to-know basis. When addressing individual inquiries, only the minimum necessary information is accessed to deliver the service.

Data Access and Logging:

- **Access Logging:** All access to data is logged in the database, including entry, duration, and activity.
- **Backup:** The database is backed up to an encrypted backup provider, AWS.
- **Transparency:** Data sharing is transparent from the onboarding stage. Users receive an invitation to join the platform, which includes links to my mhealth's Privacy Policy and Terms and Conditions. Users must read and accept these documents before proceeding.

Privacy and Terms Documents:

- Privacy Policy
- Terms and Conditions

PATIENT DATA Collection and Access:
Patient data is collected directly from patients using the service. Access is granted via individual accounts with login credentials chosen by the user, validated through Two Factor Authentication or NHS login. Clinical team members can add or amend limited data in patients' accounts, such as observations and medication changes, following interactions with the patient.

Data Relationships and Roles

Explicit relationships and the legal basis for processing are detailed Privacy Policy. This section serves to highlight the three key areas of our relationships.

The Relationship Between Healthcare Professionals and Users:

- **Healthcare Professionals as Data Controllers:** When healthcare professionals enter data or communications into the platform, they act as the Data Controller. my mhealth (MMH) serves as the Data Processor under the Data Controller's lawful basis for processing, in accordance with Article 6(1)(e) (performance of a task carried out in the public interest) and Article 9(2)(h) (processing of special category data) for processing special category data.
- **MMH as Data Controller:** For data entered by healthcare professionals on behalf of patients (e.g., blood pressure readings), MMH remains the Data Controller to deliver the agreed service, as per Article 5(1)(b) (purpose limitation) and Article 5(1)(c) (data minimisation).
- **Joint Controllers:** When healthcare professionals view patient data within their clinician account, they act as Joint Controllers with MMH for the data entered into the service, as outlined in Article 26 (joint controllers).

The Relationship Between the Procuring Organisation and my mhealth:

- **Procuring Organisation as Data Controller:** The procuring organisation, which provides access to the clinical dashboard, is the Data Controller for Clinical Team Members' information within the dashboard. MMH acts as the Data Processor, with contractual arrangements to manage this relationship under Article 28(3) (processor obligations).
- **Contractual Arrangements:** MMH processes data under the healthcare group's lawful basis as per Article 6(1)(e) (performance of a task carried out in the public interest) and Article 9(2)(h) (processing of special category data).
- **Contract Expiry:** Upon contract expiry, access to the clinical dashboard is revoked. However, patients retain access to self-manage their conditions, and MMH maintains data controllership in accordance with the specified roles, ensuring compliance with Article 5(1)(e) (storage limitation).

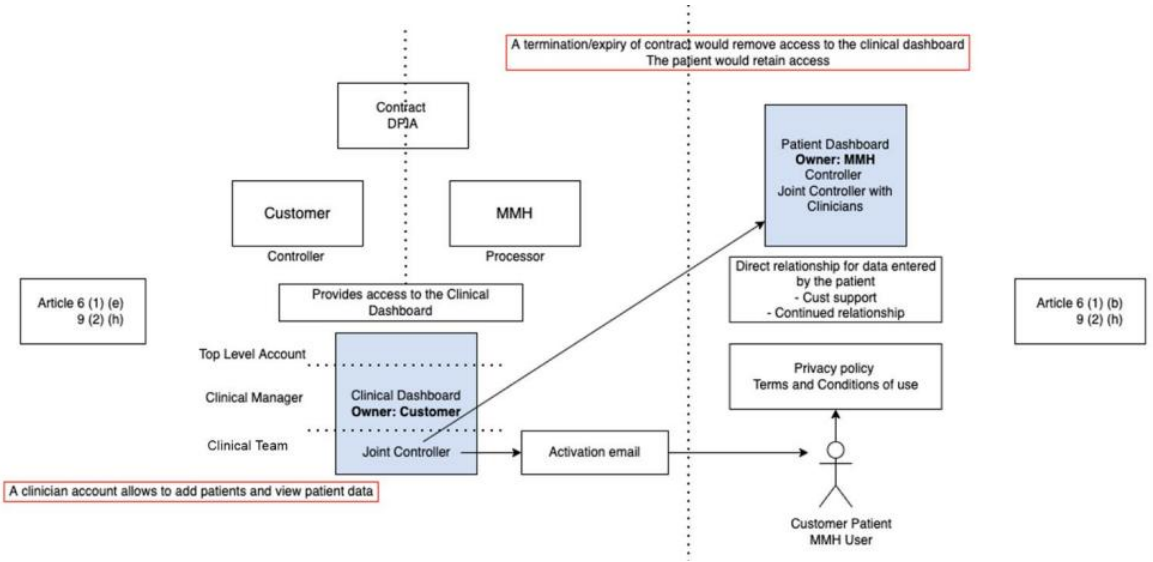
The Relationship Between the End User (Patient) and my mhealth:

- **Direct Relationship:** Once patients accept the terms and conditions and privacy policy, a direct relationship is formed with MMH.
- **MMH as Data Controller:** MMH assumes the role of Data Controller for any patient data entered into the platform. Clinical team members entering patient information during

onboarding are Data Controllers for this information, with MMH acting as their Data Processor until the user gains access to the platform. MMH's lawful basis for processing is Article 6(1)(b) (performance of a contract) and Article 9(2)(h) (processing of special category data).

- **Legitimate Business Interests:** For certain activities, MMH may process data under Article 6(1)(f) (legitimate interests), as stated in the Privacy Policy.
- **Compliance with GDPR:** MMH is committed to complying with individuals' rights under GDPR. The Privacy Policy provides transparency on data usage, processing, and duration, in accordance with Article 13 (information to be provided to data subjects). Processing of user data is as expected for the service(s) offered and does not include processing of vulnerable individuals. myAsthma is available to individuals over the age of 12. Details are provided in the my mhealth Privacy Policy, in compliance with Article 25 (data protection by design and by default).

This is shown below:



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 data deletion as permitted under GDPR. These requests will be processed by our support team, and users will be notified once their request has been completed.

The right to erasure is specifically addressed here; deleting the application from a device will not remove data stored within the platform. Patients can request edits to their data, and 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 removed, and data will be retained in accordance 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.

Does the processing achieve your purpose?

We have set out the ways my mhealth may use and process personal information and sensitive personal information, and in each case, we have noted the lawful basis and conditions that we rely on to do so.

What information will you give individuals?

- Patients are informed about the types of personal data collected, including but not limited to, health information, contact details, and usage data.
- The purposes for which their data is collected and used, such as to manage user accounts, improve service quality, and fulfil legal obligations.
- How their data is processed, including the lawful bases for processing under applicable data protection laws.
- Information on who has access to their data, including whether it is shared with third parties, such as healthcare teams or researchers, and under what circumstances.
- The duration for which their data will be retained and the criteria used to determine this period.
- The process for data anonymisation and the conditions under which data may be kept for research purposes after the retention period.
- The rights patients have under data protection laws, such as the right to access their data, request corrections, or seek deletion.
- How patients can exercise these rights, including contact information for the Data Protection Officer and procedures for submitting requests.
- The security measures in place to protect their personal data from unauthorised access, including encryption, access controls, and monitoring practices.

How will you help to support individuals rights?

We are committed to supporting individuals in exercising their rights under GDPR. For detailed information on how we manage personal data, individuals can review our privacy practices and their rights by referring to my mhealth's Privacy Policy. This policy outlines how we protect personal data, how users can access their data, and how they can request amendments or deletions.

What is your lawful basis for processing?

For more detailed information on how my mhealth handles personal data, please refer to my mhealth's Privacy Policy.

Lawful Basis for Processing Personal Data

- The purpose of creating, registering, and managing user accounts for the app(s) and service(s) provided by my mhealth is to facilitate the setup and maintenance of user access. In this context, my mhealth acts as a joint controller with the user's healthcare team, relying on contract performance as the lawful basis.
- To ensure users are informed of any changes, modifications, or updates to the app(s) and service(s), my mhealth relies on legitimate interests. This approach ensures that the services remain aligned with user needs.
- In addressing and resolving issues that may affect the use of the app(s) and service(s), my mhealth utilises legitimate interests to maintain safety and security for all users.
- To assess and improve the quality of the app(s) and service(s), my mhealth conducts troubleshooting, data quality checks, functional testing, security testing, and statistical analyses. This is also based on legitimate interests to uphold high standards.
- Maintaining accurate and up-to-date records is crucial, and for this, my mhealth acts as a joint controller with the user's healthcare team. The lawful basis is legitimate interests, ensuring the provision of relevant content and services.
- Fulfilling legal, regulatory, and risk management obligations, including reporting and disclosure requirements, is based on legal obligations.
- Preventing fraud is another key aspect of my mhealth's operations, supported by legitimate interests to protect the integrity of the services.
- To protect the rights of third parties, my mhealth adheres to legal obligations and legitimate interests, including cooperation with law enforcement and regulatory authorities as necessary.
- For enforcing legal rights, my mhealth relies on legal claims and obligations.
- Data anonymisation is carried out to ensure that information cannot identify individuals or be linked back to them. This enables sharing of non-identifiable data with researchers to support scientific research and the development of better guidelines and treatments. This is based on legitimate interests.
- When sharing information with healthcare teams via the app(s), my mhealth acts as a joint controller with the user's healthcare team. The lawful basis is contractual performance, aimed at supporting the management of medical conditions.

- Contacting users about clinical studies or research trials relevant to their conditions is done based on consent, including where sensitive personal information is processed.
- Similarly, contacting users regarding service evaluations, studies, or trials run by my mhealth is based on consent and legitimate interests.
- Reviewing users' progress through educational materials and courses within the app(s) is essential for contract performance and to provide optimal content and user experience, supported by legitimate interests.
- Understanding how users interact with the app(s) and website, including the most visited areas, helps in managing medical conditions effectively. This is based on legitimate interests.
- To comply with legal and regulatory requirements, including disclosures to government, regulatory, or law enforcement agencies, my mhealth relies on legal obligations. When feasible or where it would not hinder crime prevention or detection, any such requests are directed to the individual or they are notified prior to responding.

Will reports be generated? If yes, will the information be identifiable or anonymous (will the reports be used for research)?

Reports may be generated as part of evaluations undertaken by my mhealth and its users. These reports will be based on aggregated, anonymised data and will not contain identifiable information. However, for Human Research Authority (HRA) approved research, reports may include identifiable data but only with ethical and regulatory approval and explicit informed consent from users.

Can users request their data to be removed?

Yes, users can request data removal in accordance with their GDPR rights. These requests will be processed by our support team, and users will be notified once completed. Note that this specifically addresses the 'right to erasure'; deleting the app from a device will not remove data stored within the platform. Users can contact our Customer Support team via the (?) Support symbol on their homepage or through the 'Contact Us' section on our website. Data removal requests can also be made through the 'My Account' section of their app.

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 will be prevented through strict contractual agreements for distributed products and by ensuring that training sessions cover relevant product functions comprehensively.

How do you intend to ensure data quality?

Data quality is ensured through multiple layers of verification:

- Clinical team members manually verify data during regular patient visits.
- Patients can access their web app to verify and update their data.
- On the IT development side, we employ source control, unit testing, integration testing, and regression testing. A management structure oversees change requests and conducts code reviews to maintain data quality and accuracy.

What safeguards are in place for international data transfers?

No international data transfers are made.

Does the app send any direct electronic messages, including emails, text messages, or reminders?

The app sends in-app automated reminders, such as medication reminders, and notifications about relevant national awareness days. Upon initial registration, users receive an activation email with instructions to set up their account. Activated users will receive automated reminders at 7, 14, and 28 days. Users can toggle off in-app notifications if they prefer not to receive them.

What will happen to the information if the organisation/service ceases?

If my mhealth ceases operations, patients will have privacy controls to manage their data. They can grant or revoke access to other NHS clinical teams. Specific migration procedures will be negotiated before decommissioning infrastructure. It is likely that patients will be able to download their information before the service ends.

What measures do my mhealth implement to prevent unauthorised access to systems from outside of the company?

Encryption: All data is encrypted both in transit and at rest to safeguard against interception and unauthorised access.
DDoS Protection: AWS Shield is employed to protect against Distributed Denial of Service (DDoS) attacks.
Content Security:

- Content Security Policy (CSP) is enforced to prevent cross-site scripting (XSS) attacks.
- Secure and HTTP-only cookies are used to protect session data.

Authentication and Password Security:

- Authentication cookies are encrypted and salted.
- Passwords are hashed using PBKDF2 to enhance security.

Data Filtering and Storage:

- Incoming data is filtered using OWASP sanitisation to prevent injection attacks.
- HTML and application code are not stored in the database to mitigate risks.

Cache and Token Management:

- Data caching in web browsers is disabled to prevent sensitive data exposure.
- Tokens sent to users expire either in 3 hours or upon first use.

Password Lockout Policy: Implemented to thwart brute-force attacks.
Monitoring and Alerting:

- Prometheus and Grafana are used for real-time monitoring and alerting on cluster utilisation, enabling rapid response to activity surges.
- Alerts are sent to the DevOps team if any limits are breached. The cluster is largely self-healing, reducing the need for manual interventions.
- Daily manual and documented cluster health checks, including dashboards and logs, are performed to pre-empt potential issues.

Incident Management:

- Issues and incidents are discussed and prioritised during daily stand-up meetings and addressed accordingly.

Security Testing:

- Regular external penetration tests and vulnerability scanning are conducted to identify and address potential security vulnerabilities.

In the event of cloud service contract termination, is there an agreement and demonstration of systems to ensure that data will be transferred to another acceptable location?

Yes, we maintain full control of our data. According to the AWS customer agreement link, AWS is required to provide us with 30 days' notice in the unlikely event of contract termination. This ensures that we have adequate time to transfer our data to another acceptable location.

In the event of cloud service contract termination, is there an agreement and demonstration of systems to ensure that, following successful data transfer, data will not persist in the original cloud storage?

Yes, we have agreements in place to ensure that, following the successful transfer of data, the data will be removed from the original cloud storage. Detailed procedures and assurances are documented to guarantee that data is securely deleted from the original storage once it has been transferred.

Are there robust systems in place to prevent unauthorised access or unintended/accidental leakage between different customer environments?

Yes, AWS employs stringent measures to prevent unauthorised access or unintended leakage between customer environments. Customer accounts are segregated to ensure that data remains isolated and secure.

How quickly will the cloud provider react if a security vulnerability is identified in their product?

We use AWS Managed Services, which offer 24/7 proactive monitoring and incident management. For more details on their response capabilities, please visit AWS Managed Services.

Service Level Agreement

Is available via our website

Consultation and 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

Consultation Considerations:
When procuring a service, it is crucial to identify and consult relevant stakeholders. Consider consulting:

- **Information Governance Teams**
- **GPs (General Practitioners) and Clinical Practices**
- **Locations where the service is being procured** (e.g., regions within an Integrated Care Board (ICB), Integrated Care System (ICS), or Integrated Care Team (ICT))

Internal Stakeholders:

- Ensure you consult all relevant internal stakeholders, particularly those responsible for information security.
- If a data processor is involved, request information and assistance from them as needed. Contracts with data processors should include provisions to assist with such consultations.