my mhealth

Data Protection Impact Assessment

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.

Document control
The controlled copy of this document is maintained in the my mhealth corporate network. Any copies of this document held outside of that area, in whatever format (e.g., paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Classification: Public

Contents

General Information *3*

Supplier Information *4*

Product Information *6*

Product Benefits examples *8*

Consultation and Contacts *15*

Assess necessity and general questions *16*

my mhealth Service Level Agreement (SLA) *21*

General Information

Name of the Project	Deployment of my mhealth application(s)
Describe the purpose or aim(s) of the project	myCOPD, myHeart, myAsthma, and myDiabetes (and their derivatives) are a suite of web-based application(s) developed by my mhealth Limited, to support patients to self-manage their condition(s), enabling clinical team members to manage patient populations remotely at scale throughout the entire care pathway. The aim is to allocate licences to patients diagnosed with one or more of the supported chronic conditions (subject to contracted access), to encourage better self-care away from a clinical setting, through use of the app(s). The my mhealth mission is to improve patient outcomes and reduce healthcare costs by engaging, educating, and empowering patients and enabling clinical teams to deliver new models of care, at a population scale. **Healthcare system experience** my mhealth have market leading engagement with the NHS, growing users on a monthly basis. my mhealth have a proven track record of securing grant funding, such as SBRI and Innovate UK, and completing trials generating compelling evidence supporting the use of the platform. **Impact of services** my mhealth have a range of clinical trial data demonstrating the efficacy of the platform. This includes demonstrating that the online rehabilitation has similar impact to face-to-face programs at a fraction of the cost, users can expect significantly reduced exacerbations/re-admissions to hospital whilst correcting over 90% of inhaler errors. This is supported by compelling real-world data showing comparable outcomes in our online Cardiac and Pulmonary Rehab to standard offerings, and excellent post market surveillance from numerous independent sources stating users find the platform easy to use, and that they would recommend it to others.

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 Registration number: **ZA151364** Expiry month: November (auto renews by direct debit)
Is the supplier compliant with the Data Security Protection Toolkit? Next required Completion:	Yes Last Completed: June 2023 Status: Exceeding Standards By June 2024
Is the Supplier DTAC compliant?	Yes
Does the Supplier have any accreditations or certifications?	Yes, please see these below. Cyber Essentials available via this link https://registry.blockmarktech.com/organisations/GBLTD07881370/ **Cyber Essentials** Certificate Number: 20d21c58-21f4-48f5-ae13-47a29c5d66c5 **Cyber Essential +** Certificate Number: f1608d39-995e-4ea1-93ff-19ba3e62aecf **DCB0129** Assured by Safehand **ISO 13485:2016** Medical devices — Quality management systems
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 2 factor authentication or via NHS login
Does the Supplier appear on any commercial Frameworks?	Yes, DPS Spark, The London Procurement partnership, HSSF, GCloud12 Lot 2
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. Contractors sign a data sharing agreement stating that any transmission and use of the data is forbidden and only system operations are allowed.

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?	We have a customer support team, customer success and operations divisions to ensure support to customers. The level of support can vary dependant on the chosen package option
Does the supplier have measures in place to ensure continued trade from suffering a disaster?	my mhealth have an embedded and tested disaster recovery plan. This was most recently tested throughout the global pandemic.
Does the Supplier have information security policies?	Yes. my mhealth information security policies include: • Encryption of personal data on desktop computers and devices • Encryption of personal data on storage devices and backup • Controls against denial-of-service attacks • Controls against hacking • Clear Desk and Clear Screen
Does the supplier have a data breach Policy? How will data breaches be reported? Does the supplier keep records of all Data breaches?	Yes. my mhealth Limited will alert the designated contact of a breach. Where applicable, my mhealth will file the breach at NHS / DSPT (Data Security and Protection Toolkit) reporting tool and report to the ICO (Information Commissioners Office) (Information Commissioners Office). Yes

<table>
<tr><th colspan="2">Product Information</th></tr>
<tr><td>Category of product</td><td>Software as a service (SaaS)</td></tr>
<tr><td>DTAC Assessed?</td><td>Yes</td></tr>
<tr><td>Registered with the MHRA (Medicine and Healthcare Research Authority) as a medical device?</td><td>Yes
Class I
Reference: 6169</td></tr>
<tr><td>Service example</td><td>Video examples of the platform can be found on the mymhealth website

myCOPD <b>here</b>
myHeart <b>here</b>
myDiabetes <b>here</b>
myAsthma <b>here</b></td></tr>
<tr><td>Does the platform bear a UKCA marking for quality and safety</td><td>Yes, this can be viewed on the supplier website www.mymhealth.com</td></tr>
<tr><td>Supported web browser versions?</td><td>We support the most recent (N) and the two previous (N-2) versions of these browsers unless otherwise indicated.
<table>
<tr><th></th><th>Chrome</th><th>Firefox</th><th>Safari*</th><th>Edge**</th></tr>
<tr><td><b>Android</b></td><td>☑</td><td>☑</td><td></td><td></td></tr>
<tr><td><b>iOS</b></td><td>☑</td><td>☑</td><td>☑</td><td></td></tr>
<tr><td><b>Linux</b></td><td>☑</td><td>☑</td><td></td><td></td></tr>
<tr><td><b>macOS</b></td><td>☑</td><td>☑</td><td>☑</td><td></td></tr>
<tr><td><b>Windows</b></td><td>☑</td><td>☑</td><td></td><td>☑</td></tr>
</table>
* WebRTC support in Safari started with Safari version 11
** We support Chromium-based Edge only. Legacy Edge isn’t supported.

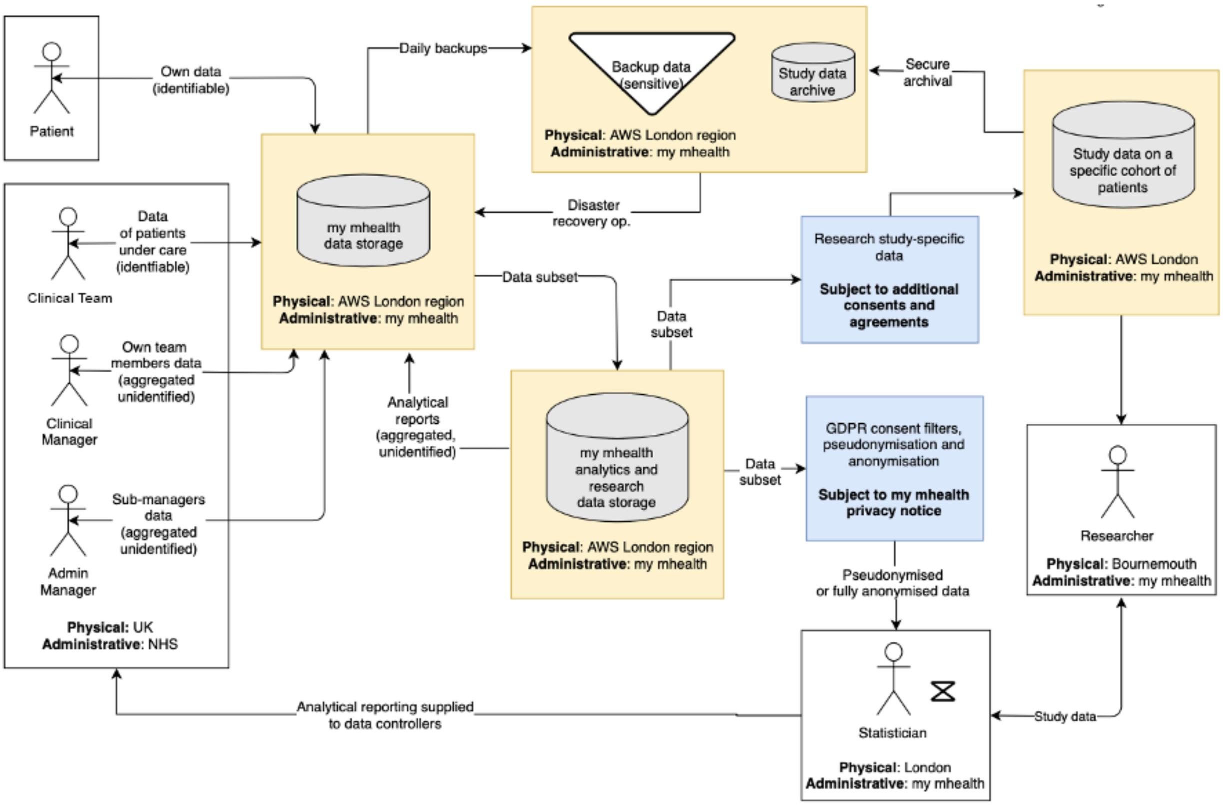
<i>For security reasons we recommend using the latest versions available.</i></td></tr>
<tr><td>Are any browser plug-ins required?</td><td>No additional software is required, such as Flash or Java</td></tr>
<tr><td>Are there any technical requirements to</td><td><b>For users;</b>
a) Download the my mhealth app from Play Store or Apple Store;</td></tr>
</table>

implement the service?	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

Patient	Clinical Team Members
• Easy-to-follow educational videos to learn how to manage their condition • Complete online education such as pulmonary rehabilitation courses • Reports can be generated to show changes in symptoms over a period of time • Weather and pollution forecasting - Receive an accurate forecast daily to understand how the weather and air pollution in local areas can impact health. Plan the day with confidence • Notifications to inform patients of medication reminders, to advise of any changes made by their clinician or if their clinical team has sent them a message. • Medication Management (Medication Diary and My medications) View, add and delete functions. With prescription assessment according to national guidelines. Medications can only be added if condition specific. • Self-management plan and diary- Know when, and how to take your medication with the online, self-management plan. The person can also record when they have taken their treatment in the medication diary. This is real time user contributed data that can be viewed in the clinical portal. • How to use sections- Global guidance on how to use the app, in addition to how-to-use videos available on each function. • Upload information / photos to support shared decision making e.g., diabetes eyes, kidney and foot care • Walking- Videos of varying length that a patient is able to follow at their leisure at home • Activity Diary-Tracking physical and rehab activity. Additional functionality to connect to selected integrated fitness devices via Bluetooth to allow seamless automated data capture.	• The clinical dashboard enables clinical team members to deliver self-management, education, inhaler technique training and education courses e.g., pulmonary rehabilitation course on any smartphone or tablet or browser. Each intervention has been shown to deliver the same outcomes as access to a face-to-face education e.g., rehabilitation class and correct 98% of inhaler errors and enables you to manage your patients like never before. • Real-time patient symptom tracking • View prescriptions against national guidelines, check medication conflicts and assess overall monthly cost of prescriptions. • The videos e.g., inhaler videos can be used to update own education or use the video button to deliver education to the user at their community or clinic visit. **System benefits:** • Reducing variations of care • Increasing resilience of workforce teams • Supporting patients at home

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;


Patient
Own data (identifiable)
Daily backups
Backup data (sensitive)
Study data archive
Physical: AWS London region
Administrative: my mhealth
Secure archival
Study data on a specific cohort of patients
Physical: AWS London
Administrative: my mhealth
Clinical Team
Data of patients under care (identfiable)
my mhealth data storage
Physical: AWS London region
Administrative: my mhealth
Disaster recovery op.
Research study-specific data
Subject to additional consents and agreements
Data subset
Data subset
Clinical Manager
Own team members data (aggregated unidentified)
Analytical reports (aggregated, unidentified)
my mhealth analytics and research data storage
Physical: AWS London region
Administrative: my mhealth
Data subset
GDPR consent filters, pseudonymisation and anonymisation
Subject to my mhealth privacy notice
Researcher
Physical: Bournemouth
Administrative: my mhealth
Admin Manager
Sub-managers data (aggregated unidentified)
Physical: UK
Administrative: NHS
Pseudonymised or fully anonymised data
Statistician
Physical: London
Administrative: my mhealth
Analytical reporting supplied to data controllers
Study data

Patient data, both identifiable and special category data is collected directly from patients using the service. This is entered via an individual account controlled by log in credentials chosen by the user or via NHS Login. There is multi factor authentication with an email address and password. (aligning to my mhealth password policy). Clinical team members are also able to add data such as observations and medicine changes following an appointment with the patient.

Clinical team data is collected by their top level account and clinical manager accounts. Clinical team members are also provided with in an individual account as part of the clinical dashboard, accessed via their email address and their chosen password (aligning to my mhealth password policy). This is enabled with Multi Factor Authentication. my mhealth do not use this data but do incorporate it into aggregated anonymised performance data which is reported back to clinical teams as agreed contractually.

Data is stored within Amazon Web Services London Regions only. A cloud service database cluster over 3 separate locations for fewer down time hours. Each region of our infrastructure is fully partitioned/isolated with availability zones (AZ), to better isolate any issues and achieve high availability. Each AZ (London) has its own power infrastructure and is connected with a fast, private fibre-optic network. Amazon Web Services London are made up of a cluster of Tier-4 connected data centres.

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

We use the collected data to:

To provide the service

This is to be able to give access to the service and to register and manage user accounts. To inform users of any alterations, modifications, and updates to the service and to review, investigate and address issues that may affect the use of our service.

To exercise our legitimate interests

We will use data to review and assess the quality of our service and make improvements. We need information to provide a responsive service to both patients and healthcare professionals a responsive support service. This is via our customer support team.

We will also use information for internal operations. These might include troubleshooting and resolution, data quality checks, functional testing, security, audit and statistical analysis to ensure that our app(s)/service satisfies the requirements of our users. This is through the use of anonymised data only.

To consent to receiving information around research opportunities

my mhealth participates in research. As part of our privacy policy, (patient) users are asked if they would consent to receiving information about research opportunities. Users are free to review the information and participate or not without it affecting their access to or functionality of their app.

To respond to obligatory requirements

We will disclose information if we are requested to do for a regulatory requirement or in response to a legal request

The service is a support tool, for users to record symptoms, learn more about their condition(s) and improve patient self-management. To do this, information is **shared** in the following ways:

1) Data back-up services (AWS) are our third-party supplier to back up the information entered into an account. AWS can see identifiable data if they are required by law, otherwise there is no visibility of this data. This is controlled via contractual agreements with AWS.

2) Push notification software providers to communicate medication reminders and updates from healthcare teams. This functionality is to assist the patient to ensure adherence to their medication plans and for clinicians to communicate via the in-app functions.

3) Healthcare & research teams to evaluate the service provided. We will also take part, via our designated research team, where approved by the relevant authorities in assisting with studies, evaluations and medical research. This is to help understand more about the condition(s) and the improvement of future treatments. my mhealth do ask for explicit consent for this option via the privacy policy (see above).

4) SMS messaging services for communicating to/with you, information relevant to your condition(s). These are providers where the healthcare teams have already received prior approval, for the use of these systems.

This is managed by a **contract** between my mhealth Limited and their customers', which include data governance clauses and a Service Level Agreement (SLA). Sharing of user data is managed by the privacy policy www.mymhealth.com/privacy.

Access to Personal and special category data:

Patients are able to access their own data

Clinical team members are able to access data of patients under their direct care

Clinical Managers and Top Level accounts are held by our Operations division. There is no patient data available at these levels and this functionality is to support administrative set up for Clinical teams, reducing time burden. Holders are able to access anonymised and aggregated data only.

At my mhealth, access is limited to named, designated full-time employees holding contract confidentiality clauses on a need-to-know basis. When dealing with individual enquiries, we will only ever access the minimum information necessary to deliver the service.

ACCESS IS LOGGED IN THE DATABASE. Entry length of time and activity and the database is backed up to an encrypted back up provider - AWS

The sharing of data is transparent to the user from the onboarding stage. Users are added to the system which triggers an invitation to join the platform.

This link present users with my mhealth Privacy Policy and the Terms and Conditions of use for the service. These have to be read and accepted to before the user is able to move on. These documents can be found on the my mhealth website or by the following links;

mymhealth.com/privacy
mymhealth.com/terms

DATA IS RETAINED in line with the guidance printed by the National Health Service of '*Record of long term illness or an illness that may reoccur*' within the Records Management Code of Practice for Health and Social Care 2021 pages 56 –Long-term conditions management, and 70 – research datasets.

https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf

We hold patient data for a period of 20 years, from the last patient activity, unless we are notified by either the healthcare team or a relative of the patient of their passing, and data will then be anonymised after 10 years from the date of death. After 20 years the data will be anonymised in line with article 5 (e) of the of the General Data Protection Regulation UK (GDPR UK) and used only for clinical research or statistical studies. This will not be able to be re-identifiable and scripts are written within the service to trigger the data to be anonymised and archived. All identifiable data is removed from the my mhealth platform at the retention period. All data that has been anonymised in line with Article 5, is stored within the my mhealth insights platform.

Users can opt out of communications and can request to be deleted, where their rights under the GDPR UK allow. We will action these requests via our support team and update users when this has been completed. This is specifically for 'the right to erasure' as deletion of the application from devices will not delete data within, as per any other app individuals may use. Patients can request edits to their data and clinical team members can also edit limited amounts of data via either a web browser or the my mhealth app, but only for users that sit within their own account structure and not that of users outside of their dashboard.

If services are NO LONGER REQUIRED, THE CONTRACT EXPIRES OR IS TERMINATED access to the clinical dashboard will be removed and the data within would be retained in line with the my mhealth data retention policy as shown above.

my mhealth have embedded management systems in place to ensure the security and quality of its systems and the data within. All data collected, processed and stored is done so utilising AES-256 encryption in transit and at rest. The transfer of data is via network only Transfer layer Security (TLS) 1.2 only. This includes the transmission of data from the my mhealth interface to the back up and system host (AWS) remote access to infrastructure holding patient data is monitored on a daily basis and the company complies with the requirements for the DSPT and the DCB 0129. As part of the management systems there are policies for physical access control and mobile work/acceptable use of devices, as well as delivery of sensitive access details.

The CLINICAL RISK SAFETY (DCB 0129) is managed by the company's Medical Director, and assured by Safehand and ALL clinical guidance and references within the platform are aligned to NICE (NATIONAL INSTITUTE FOR HEALTH AND CARE EXCELLENCE) OR NATIONALLY ACCEPTED guidelines. Details on Clinical Safety are outside the scope of this document and can be obtained separately.

NETWORK AND SYSTEMS SECURITY

Data in transit: Restriction to TLS v1.2 only, using updated, secure ciphers (AES 256 where possible). Known insecure protocols, ciphers and configurations are disabled, e.g., RC4, SSL3, non-perfect-forward secrecy, client re-negotiation.

Ciphers utilised for data in transit are:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Operational work involving security: systems security patching, internal and external security audits, software quality assurance process and application security updates as part of the software development lifecycle, policies on network configuration, security advisory reviews covering full stack software components, IT staff training on security.

PHYSICAL SECURITY

Hosting infrastructure: my mhealth Limited are not permitted to disclose further information on the hosting infrastructure. Please refer to AWS Artefact service to obtain compliance documents under a Non-Disclosure Agreement (NDA).

my mhealth operates a fully remote working environment with cloud-based hosting software and therefore have no physical premises. All employees receive cyber security and information governance training annually at minimum, and are governed by a series of homeworking policies and procedures, that include bit not limited to; clear desk policy and acceptable use policy.

APPLICATION SECURITY

Content Security Policy (CSP), secure cookies and HTTP-only cookies are enforced in HTTP communications. Authentication cookies are encrypted and salted. Passwords are hashed utilising PBKDF2. Incoming data are filtered using OWASP sanitisation at point of reception. HTML and application code are disallowed as content in the database. Data caching is disabled in web browsers. Tokens sent to users expire in 3 hours or when utilised a single time.

Operational security on the development side includes separation of testing and production environments (including no secrets in source control), IT Change Management procedure on information assets including documented procedures for development, functional and non-functional testing. Security code reviews are routinely made, and all code changes are logged in a version control system.

VIRUSES AND MALICIOUS CODE protection are implemented as a layer approach.

At data level, the system utilises OWASP components to filter all incoming and outgoing data against malicious code.

At a deployment level, we regularly review our projects in Dependency Track (https://dependencytrack.org/) and our AWS Elastic Container Registry (ECR) image scanning results and apply fixes as necessary.

my mhealth maintains its annual assessment for the **Cyber Essential Plus** certification and completes an annual external accredited PENETRATION TEST on the platform, followed by quarterly vulnerability scans. All identified issues are resolved regardless of their severity.

The data collected through the service is personal identifiable and special category health data. This is required for the service to deliver its intended purpose and is limited to the minimal amount needed to use it. Below is a summary covering all disease applications.

From patients (sensitive and Special Category Health Data):

Basic contact details, name address, symptoms, medication commitment, location (GPS and/or postcode. This can be switched off by the user on their device like any other application), disease details and metrics, research analytics data including video usage, login details, device information (for service evaluation and improvements)

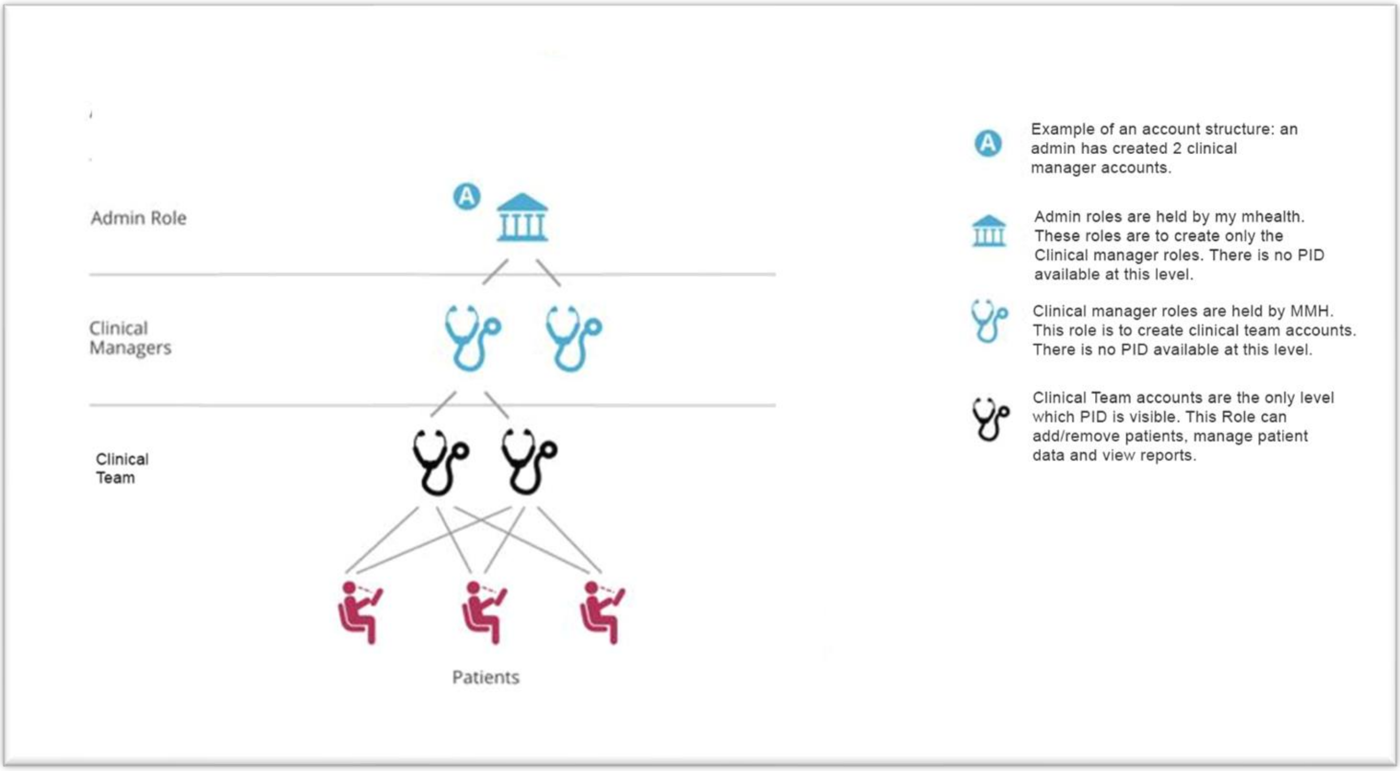
PID (Personal Identifiable Data): Patient's clinician, next of kin and GP contact details.

Special category data: Data relating to individuals' health is entered by the patient directly into the system. These are general wellbeing and symptoms relating to users' health.

From Clinical team members (corporate):

Name, role, email address, telephone number, organisation, or team name.

The service does not require criminal data collection or processing and does not lead to profiling of patients.



A Example of an account structure: an admin has created 2 clinical manager accounts.

Admin roles are held by my mhealth. These roles are to create only the Clinical manager roles. There is no PID available at this level.

Clinical manager roles are held by MMH. This role is to create clinical team accounts. There is no PID available at this level.

Clinical Team accounts are the only level which PID is visible. This Role can add/remove patients, manage patient data and view reports.

The service is intended to be utilised by the patients as a self-management tool at a frequency relevant to the patient. This will naturally depend on their condition, medication, and self-management plan requirements. The processing of data will be continuous and will scale with the number of patients onboarded to the platform. The Contractual arrangements and the above account set up will control the geographical location of the processed data. my mhealth geographical location will be within the AWS London regions.

Identifiable data and special category data are processed/retained in line with the guidance printed by the National Health Service of *Record of long-term illness or an illness that may reoccur* within the Records Management Code of Practice for Health and Social Care 2021.

We hold patient data for a period of 20 years, from the last patient activity, unless we are notified by either the healthcare team or a relative of the patient of their passing, and data will then be anonymised after 10 years from the date of death. After 20 years the data will be anonymised in line with article 5 (e) of the of the General Data Protection Regulation UK (GDPR UK) and used only for clinical research or statistical studies.

https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf

PATIENT DATA is collected is directly from patients using the service. The application is accessed via an individual account utilising log in credentials chosen by the user, validated by Multi factor Authentication or via NHS login. Clinical team members are also able to add/amend limited data in the patients' account, such as observations and medicine changes following an interaction with the patient.

There are 3 separate relationships that form part of the service;

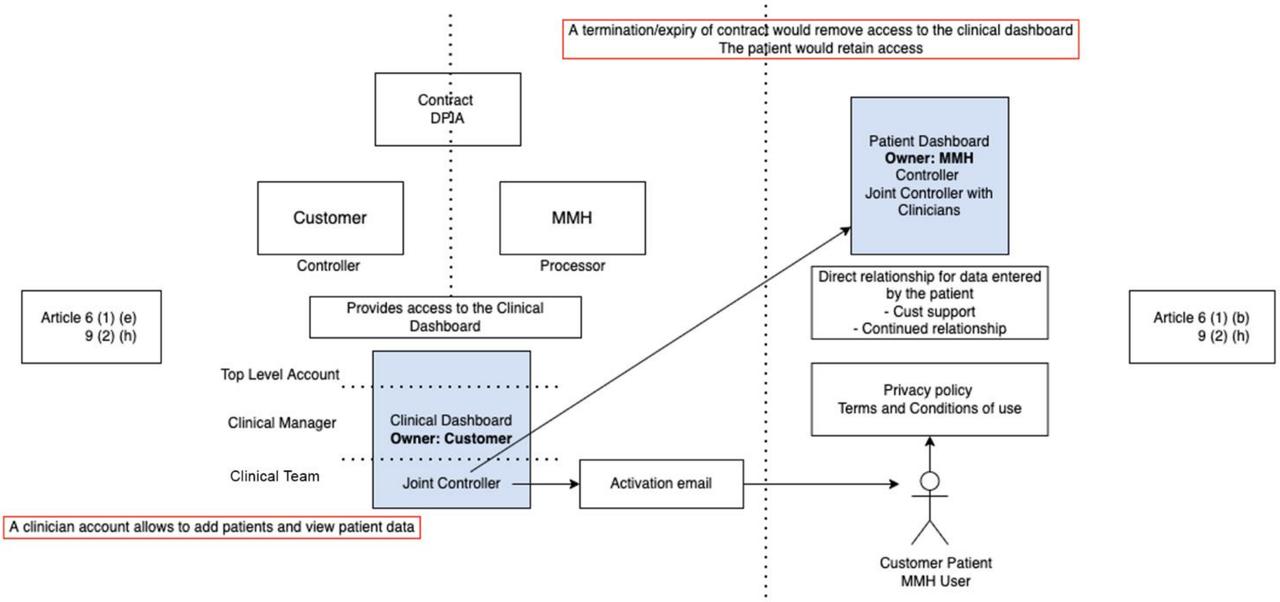
THE RELATIONSHIP BETWEEN THE HEALTHCARE PROFESSIONALS AND USERS

This relationship will vary based on the healthcare professional's capacity, at the time of data entry.

Where data and/or communication(s) are entered into the platform by a healthcare professional, the healthcare professional acts as the **DATA CONTROLLER** and **MMH (my mhealth)**, as their data **PROCESSOR** under the controllers' lawful basis for processing, Article 6 (1) (e) and Article 9 (2) (h), when processing special category data.

Where data is entered into the platform by a healthcare professional, **on behalf of the patient**, where this data would normally be entered by the patient, **MMH** remain the **CONTROLLER** of this data (such as, blood pressure or blood sugar readings), to be able to deliver the agreed service.

Where patient data is viewed by the healthcare professional(s), within their clinician account (where access has been provided via the hierarchal flow shown in the previous section), the healthcare professionals assume the role of **JOINT CONTROLLER** with **MMH** of the patient/user data entered into the service. This is shown below.



THE RELATIONSHIP BETWEEN THE PROCURING ORGANISATION AND MY MHEALTH.

This provides customers/potential customers access to a clinical dashboard, allowing an overview of their patients' care. For this relationship the **PROCURING ORGANISATION** is the **DATA CONTROLLER** for the **CLINICAL TEAM MEMBERS** information within their clinical dashboard and my mhealth act as their **DATA PROCESSOR**. There are contractual arrangements to manage this. **MMH** will be acting under the healthcare group's lawful basis of processing, as a processor under article 6 1(e) and Article 9 (2) (h), when processing special category data.

Contract expiry between the 2 organisations will revoke access to the clinical dashboard however, the patient will continue to have access to self-manage their conditions without the clinical oversight and MMH will retain data controllership, as outlined within the above relationships.

THE RELATIONSHIP BETWEEN THE END USER (PATIENT) AND MY MHEALTH.

Once the patient accepts terms and conditions and privacy policy the direct relationship and agreement is formed with the user(s). **my mhealth** assume the role of the **DATA CONTROLLER** for the/any **PATIENT DATA** entered into the platform. The **Clinical team members** entering patient information into the onboarding page (to provide the patient with the onboarding link) are the **DATA CONTROLLER** of this information and my mhealth act as their processor, up until the user obtains access to the platform. As the Data Controller MMH lawful basis for processing is 6 1 (b) for the purpose of delivering the agreed service and Article 9 (2) (h) when processing special category data. We will at times, with certain activities, be acting under Article 6 (1) (f), legitimate business interest as previously mentioned in the DPIA.

my mhealth are committed to comply with individuals' rights to their information. Individuals are able to exercise their rights under the General Data Protection Regulations. This can be viewed in the my mhealth privacy policy. www.mymhealth.com/privacy '*What rights do you have regarding your information?*' **This applies for the full retention period as outlined below;**

IDENTIFIABLE DATA IS PROCESSED/RETAINED in line with the guidance printed by the National Health Service of *Record of long-term illness or an illness that may reoccur* within the Records Management Code of Practice for Health and Social Care 2021. 20 years, from the last patient activity, unless we are notified by either the healthcare team or a relative of the patient of their passing, and data will then be anonymised after 10 years from the date of death. After 20 years the data will be anonymised in line with article 5 (e) of the of the General Data Protection Regulation UK (GDPR UK) and used only for clinical research studies.

https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf

Anonymisation of all data will occur at this point (see above), to allow for the archiving of personal identifiable and special category data. From this point, it will no-longer be possible to be re-identified and may be used for no other/additional purposes. All data is removed from the my mhealth platform at the retention period. All data that has been anonymised in line with Article 5 (e), is stored within the my mhealth insights platform.

The privacy policy also provides users with a transparent view of what their information is used for, how it will be processed, and for what duration. Processing of user data is as expected for the service(s) offered and does not include the processing of vulnerable individuals.

myAsthma is available to people over the age of 12 years old and the processing of data will be governed by GDPR.

Consultation and Contacts

Please name the individuals (and their roles) that should be involved in this process.	**Head of Compliance**: 01202 299 583, Compliance@mymhealth.com

However, if you decide this is not appropriate, you should provide a clear explanation why.	**Data Protection Officer / Caldicott Guardian/ Medical Director** 01202 299 583, DPO@mymhealth.com **Senior Information Risk Owner (SIRO)**: phone 01202 299 583, david.pettigrew@mymhealth.com
Do we need to consult anyone else? You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security. If you use a data processor, you may need to ask them for information and assistance. Your contracts with processors should require them to assist.	This should be a consideration for all customers to identify any stakeholders needing to be consulted such as (but not limited to); Information Governance Teams GP (General Practitioner) and Clinical Practices Locations where the service is being procured for (regions forming part of an ICB/ICS/ICT for example)

Assess necessity and general questions	
Does the processing achieve your purpose?	Yes, the applications manufactured by my mhealth have been through trials and evaluation able to demonstrate the benefits of digital innovation within care pathways
What information will you give individuals?	Individuals have access to our support team and the suite of e-learning and video how to use the system guides
How will you help to support their rights?	www.mymhealth.com/privacy
Your lawful basis for the processing	When acting as Data Controller, my mhealth lawful basis for processing is, **article 6 (1) b), to deliver the agreed service and article 9 (2) (h), when relating to special category data.** On occasions this could also be Article 6 (1) (f), legitimate business interest. The activation link presents the patient with the terms and conditions and privacy policy, this includes all processing activities for transparency. When acting as data processor, for the customer, my mhealth lawful basis for processing would be 6 (1) (e) and **article 9 (2) (h), when relating to the processing of special category data.**

	Health care providers, or Trusts, when acting as the controller, will be acting under article 6 (1) (e). No special Category data will be collected by my mhealth about the healthcare professionals, using the platform. For contacting users about research opportunities, my mhealth with be using explicit consent as part of the Privacy Policy. (This will be achieved through an opt-in/opt-out question).
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 that personal information 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. This restriction does not apply to the personal information you provide to us separately.
Will reports be generated from this information. If yes, will the information be identifiable or anonymous (will the reports be used for research)	Health Research Authority (HRA) approved research requests will be looked at within specific information governance processes before data can be accessed and the patient would have consented when joining the research trial.
How you will prevent function creep	Contractual agreements are in place for product(s) that are available for distribution. Training sessions will also cover the relevant product functions
How you intend to ensure data quality	Data is verified manually by clinical team members and is updated or amended as part of regular visits by the patient. Patients accessing their web app can verify and update their data.On the IT development side, there is source control, unit, integration and regression testing and a management structure signing-off change requests and performing code reviews on any software change that can affect quality and accuracy of data.

How you intend to provide privacy information to individuals	The patient is provided the terms and conditions and Privacy Policy outlining the terms of use of the system and the usage of data. This is required to be read and accepted to gain access to the service.
Safeguards for international transfers	No international transfers are made
Can users request for their data to be removed?	Users can be deleted, where their rights provided under the GDPR allow. We will action these requests when received and update users when this is completed. This is specifically for 'the right to erasure' as deletion of the application from devices will not delete data within, as per any other app individuals may use. Users can contact our Customer Support team - the options to contact us are within the (?) Support symbol at the top of their homepage. There is also a 'contact us' section on our website. Users can also request to delete their account from within their account, through the 'My Account' section near the bottom of their homepage
Does the app send any direct electronic messages? Including email text messages or reminders? Are there procedures in place for an individual's request to prevent or restrict these messages?	The app will send in-app automated reminder notifications e.g., medication reminders. We may also send in-app notifications with information about relevant national awareness days. All users will receive an initial activation email when first registered to the platform and they must follow the instructions in order to set their account up. If the user does activate their account, they will receive an automated reminder at 7,14 & 28 days. In-app notifications can be toggled off if they no longer wish to receive them.
If the organisation/service ceases what will happen to the information	Patients will have the ability to grant or revoke access to other NHS clinical teams elsewhere in the UK (United Kingdom), so this process does not involve the need of a supplier, IT staff or a specific NHS team to delete the data. Patients will be given privacy controls via their app and will be able to decide what to do with their data Regarding my mhealth Limited ceasing activity, specific migration procedures will need to be negotiated before infrastructure decommissioning. It is likely that the information would be made available for download.

What measures do my mhealth implement to prevent unauthorised access to systems from outside of the company?	All data is encrypted in transit and at rest. AWS shield is used for DDoS protection. Content Security Policy (CSP), secure cookies and HTTP-only cookies are enforced in HTTP communications. Authentication cookies are encrypted and salted. Passwords are hashed utilising PBKDF2. Incoming data are filtered using OWASP sanitisation at point of reception. HTML and application code are disallowed as content in the database. Data caching is disabled in web browsers. Tokens sent to users expire in 3 hours or when utilised a single time. A password lockout policy is also in place. We use Prometheus and Grafana to monitor and alert on cluster utilisation so that we can quickly respond to surges in activity. Alerts are sent to our DevOps team should any of our limits be breached on both. Our cluster is to a large extent self-healing, so it is rare that manual interventions are required. In addition to the automated system monitoring and alerting we preform daily cluster checks which consists of manual and documented checks of the cluster health, dashboards, and logs to pre-empt any potential problems. Any problems / incidences found are discussed and prioritised after the daily stand-up meeting and actioned accordingly. External Pentest and vulnerability scanning is also in place.
In the event of cloud service termination of contract is there an agreement and demonstration of systems to ensure that data will be transferred to another acceptable location? In the event of cloud service termination of contract is there an agreement and demonstration of systems to ensure that following successful transfer of data that the data will not persist in the original cloud storage? Are there robust systems in place to prevent unauthorised access or unintended / accidental leakage between different customer environments	We are in full control of our data. In accordance to the AWS customer agreement https://aws.amazon.com/agreement/ they must give us 30 days' notice in the very unlikely event our contract would be terminated. All our data is backed up continuously and can be downloaded in standard format and exported to a new cloud provider. Yes, please see here

in the cloud storage? How quickly will the cloud provider react if a security vulnerability is identified in their product?	AWS customer accounts are segregated. We use AWS Managed Services which provide 24/7 proactive monitoring and incident management. https://aws.amazon.com/managed-services/

my mhealth Service Level Agreement (SLA)

my mhealth Service Level Agreement (SLA) is a policy governing the availability and IT support of the systems, networks, storage and applications provided by my mhealth and its affiliates to their institutional customers.

Service constraints
To use the service, your users will need updated web browsers and updated mobile devices. Please see "Instructions for Use."

Network Service
Reasonable commercial efforts will be used to provide network service availability with a monthly uptime percentage of at least 99.95%.

Unavailability of this service means when all of the running application services have no external connectivity.

Storage Service
Reasonable commercial efforts will be used to provide availability of storage service at a monthly uptime percentage of at least 99.95%.

Unavailability of service means when all of the attached storage volumes perform zero read-write IO, with pending IO in the queue.

IT Service Support
The IT team will actively monitor the service and apply corrective measures to it during business days. A team of IT professionals will monitor the system from 08:00 until 17:00 UTC±00:00 (UK time), from Monday to Friday, except Bank Holidays.

For other regions or needs, specific arrangements will be defined in the service contract.

IT support contacts in the UK are:

Office hours: +44 1202 299 583, live chat on website or email to support@mymhealth.com
Out of office hours: email to support@mymhealth.com

Our response time for support messages is two hours during office hours.

Incident reporting
my mhealth will notify you of any relevant incident affecting the service, including service unavailability, functionality disruption, data loss or systems hacking.

my mhealth will also inform you of planned maintenance activities that potentially may disrupt the service.

Notification will be made to designated contacts of your organisation. Your organisation is responsible for keeping us updated on the designated contacts. Please write to support@mymhealth.com.

Service Recovery
Upon incident notification by the customer or automated monitoring tool, the **Recovery Time Objective** will be:

a) 2 hours during office hours and
b) 8 hours during out-of-office hours relative to the deployment location.

The **Recovery Point Objective** will be 24 hours or less depending on specific commercial agreements.

Planned Maintenance Periods
In the unlikely event of a major infrastructure update needing an outage period, we'll notify you at least 48 hours before, and will attempt to schedule the intervention for periods of low impact to the end users.

Data Retention
Please refer to the "Data Retention Policy."

SLA Exclusions
This service commitment does not apply to availability, quality, performance, correctness or any other issue in case of:

a) *Force Majeure* events

b) Events that are not directly under our reasonable control, including Internet access to our service and misconfigurations in user's devices

c) Events resulting from actions or inactions of you or any third party

d) Suspension or termination of service under the Service Contract

SLA Exceptions
Clauses that are part of a service contract may or may not override or complement this policy.