Data Protection Impact Assessment

This DPIA is provided as a resource only and is not intended to be used to identify your own risks

Document management

Version History

Version	Date	Summary of changes
1.0	14th April 2021	Initial Document

Reviewers This document has been reviewed by:

Reviewer name	Title / responsibility	Date	Version reviewed
David Hale	Head of Compliance	14th April 2021	1.0
Adam Kirk	Medical Director/DPO	14th April 2021	1.0

Approval This document has been approved by:

Name	Title / responsibility	Date	Approved version
Adam Kirk	Medical Director/DPO	14th April 2021	1.0

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.

Table of Contents

General Information	
Name of the Project	Deployment of my mhealth application(s)
Describe the purpose or aim(s) of the project	myCOPD, myHeart, myAsthma, myDiabetes are a suite of NHS-approved web-based application(s) developed by My mHealth Limited, to support patients to self-manage their condition(s), enabling clinicians to manage patient populations remotely at scale throughout all care pathways. The applications also include a six-week pulmonary rehabilitation and educational programme (s). The disease specific applications are an evidence-based intervention, which has been through several rigorous evaluation processes through the NIA, Small Business Research Initiative (SBR)I, NHS England, and has been through a series of randomised-controlled trials. The aim of the project is to allocate licences to patients diagnosed with one or more of the supported chronic conditions, to encourage better self-care away from a clinical setting, through use of the app(s).

Supplier Information	
Supplier details	My mhealth Limited
Registered address	8 Trinity, 161 Old Christchurch Road, Bournemouth, BH1 1JU
Registration number	07881370
NHS organisation code	8JH30
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: March 2020 Status: Exceeding Standards By June 2021
Does the Supplier have any accreditations or certifications	Yes, please see these below. Cyber Essential Cyber Essential +
What screening is carried out on new employees / contractors?	All existing and new employees have updated DBS 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.
Do my mhealth provide set up and ongoing support	We have a customer support team and engagement specialists 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

Product Information	
Category of product	Software as a service (SaaS)
NHS App store approved?	Yes
Registered with the MHRA as a medical device?	Yes Class I Reference: 6169
Service example	Video example of the platform can be found here
Does the platform bear a CE marking for quality	Yes, this can be viewed on the supplier website www.mymhealth.com
Supported web browser versions?	You can use a variety of browsers. Edge 13 or above; • Chrome 60 or above; • Chrome 53 for Android or above; • Firefox 60 or above; • Safari 11 or above. Internet Explorer 11 browser is still informally supported but not recommended. For security reasons we recommend using the latest versions available.
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. Internet Explorer 11 is still informally supported but not recommended. For Clinicians; Clinicians 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	Clinician
• 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 clinician has sent them a message. • 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. • Upload information / photos to support shared decision making e.g. diabetes eyes, kidney and foot care	• The clinical dashboard enables clinicians to deliver self-management, education, inhaler technique training and education courses e.g., pulmonary rehabilitation course on any smartphone or tablet. 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 to workforce teams • Supporting patients at home

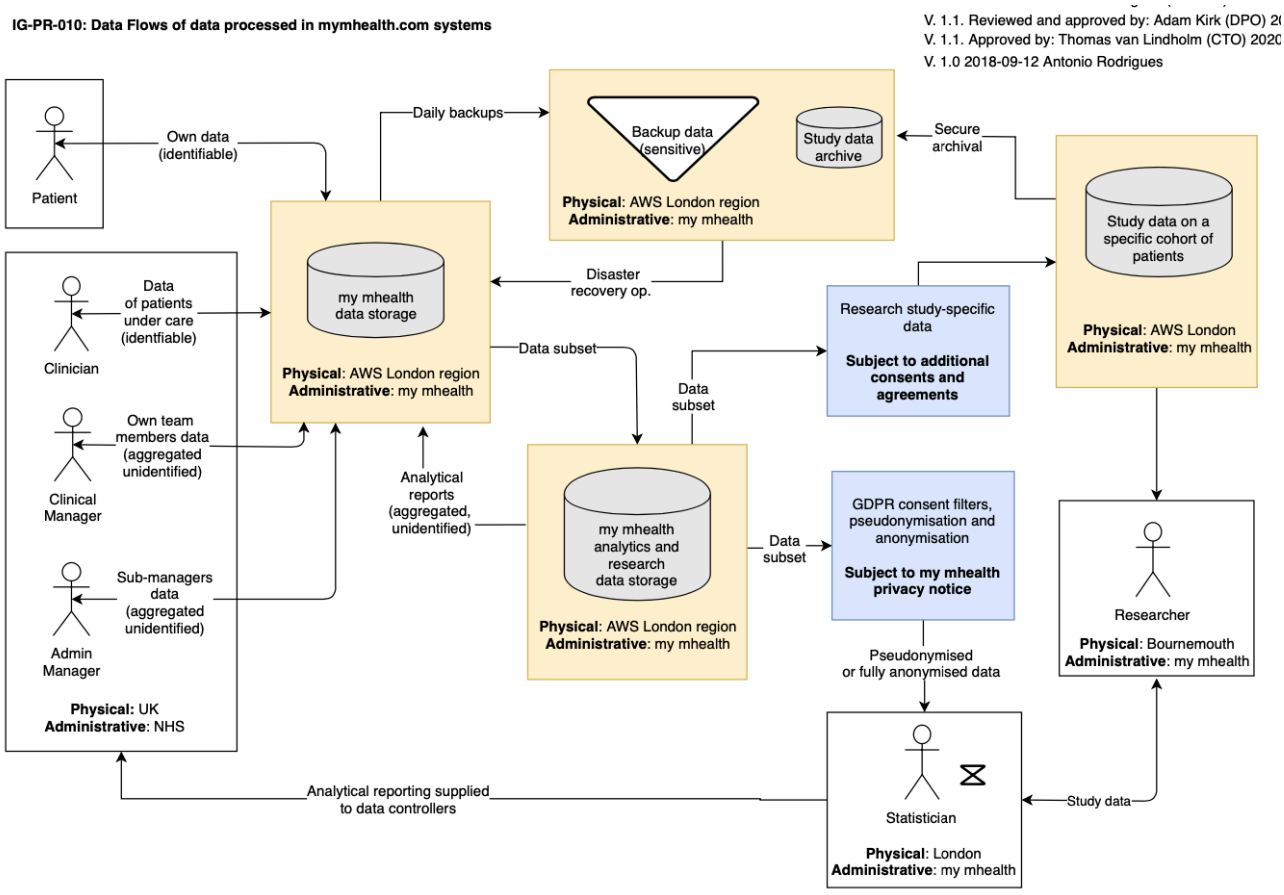
The nature of the processing.

This is what you plan to do with the personal data. This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;
- retention periods;
- security measures;
- ~~whether you are using any new technologies;~~
- ~~whether you are using any novel types of processing;~~
- ~~which screening criteria you flagged as likely high risk.~~

From the perspective of my health these are removed as not relevant

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



Patient data is collected is directly from patients using the service. This is entered via an individual account controlled by log in credentials chosen by the user. This is currently **single factor authentication** with an

email address and password. (aligning to my mhealth password policy). Clinicians are also able to add data such as observations and medicine changes following an appointment with the patient.

Healthcare professional data is collected by their commission group/trust and clinical manager accounts. Healthcare professionals 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).

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 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 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 out customer support team.

We will also use information for internal operations. These might include troubleshooting, fraud detection 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 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 are able to see identifiable data in the event that 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. This will always be anonymised unless users have provided additional recorded consent. 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. For clinical trials users are approached, without obligation, aligning to the Privacy and Electronic Communication Regulation, when these types of opportunities arise. Users are able to consent or opt out. This is simply and FYI and has no effect on the procured service.

4) SMS messaging services for communicating to you, information relevant to your condition. These are providers where the healthcare teams have already gained consent, such as MJOG.

This is managed by a **contract** between my mhealth Limited and the CCGs, 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 data;

Patients are able to access their own data

Clinicians are able to access data of patients under their direct care

Clinical Managers and Top Level are able to access anonymised aggregated data and also data input about the clinicians.

At my mhealth is limited to named, designated full-time employees holding contract confidentiality clauses on a need-to-know basis. This is the support and development team, when dealing within individual enquiries and issues. We will only ever share the minimal 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 read and accepted/consented to before the user is able to move on. These can be found on the my mhealth website or by the following links;
www.mymhealth.com/privacy
www.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 2016. We hold patient data for a period of 30 years, 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 8 years from the notification point. After 30 years the data will be anonymised in line with article 5 of the of the General Data Protection Regulation (GDPR) and used only for clinical research studies. Scripts are written within the service to trigger the data to be anonymised and archived.

Users are able to be deleted in line with their rights provided under the GDPR. We will action these requests when received and provide users 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. Patients, clinicians and healthcare managers can also edit the data via either a web browser or the my mhealth app, bit inly in the areas that their account allows access (please see the account hierarchy diagram).

If the services were **no longer required or 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 health 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, a practicing physician and ALL clinical guidance and references within the platform are aligned to **NICE** guidelines. This is the National Institution for Health and Care Excellence. 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_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_A ES_256_GCM_SHA384
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 allowed 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 offices: Keys, secrets and passwords are stored in audited, compliant encrypted vaults (AES256) and follow a Password Policy. There is CCTV in operation, with a view of the electric gated carpark, and digital key code lock in addition to 3 doors to access the premises.

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 deployment level, software build artefacts are virus-scanned using Cisco's ClamAV before deployment.

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. Further details

The scope of the processing

This is what the processing covers. This should include, for example:

- The nature of the personal data;
- The volume and variety of the personal data;
- The sensitivity of the personal data;
- The extent and frequency of the processing;
- The duration of the processing;
- The number of data subjects involved; and
- The geographical area covered.

The personal data collected by the service is the minimal amount needed to use it. Below is a summary covering all disease applications.

From patients (**sensitive**):

Basic contact details, name address, symptoms, nutritional data, 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 analytical data including video usage, login details, device information (for service evaluation and improvements)

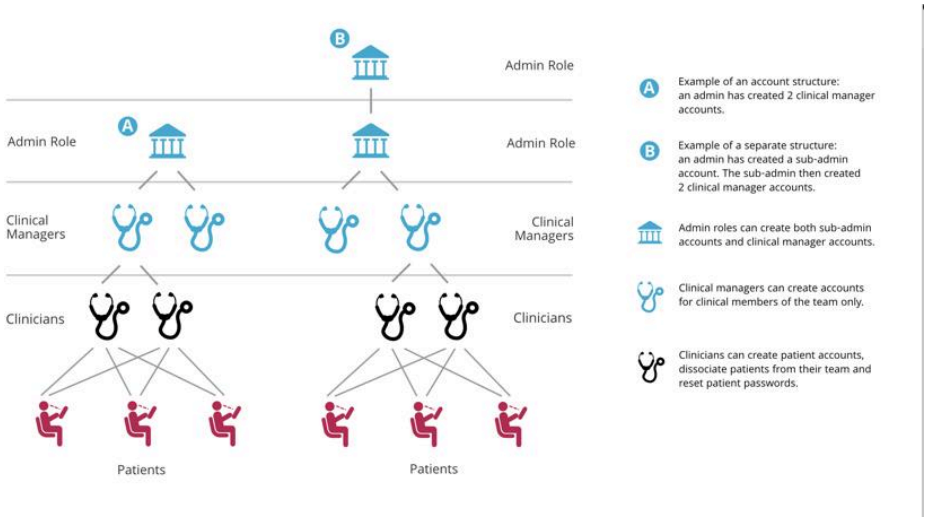
PID: patient's nurse, next of kin and GP contact details.

From clinicians (**corporate**):

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

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

From administrative roles, such as the CCG/Trust top level account holder involved in the licence distribution (**corporate**): name, role, email address, telephone number, organisation or team name. This is because this will be the overall contact. Please see the account hierarchy diagram for reference.



The service is intended to be utilised by the patients daily, at minimum. 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. The my mhealth geographical location will be within the AWS London regions.

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 2016. We hold patient data for a period of 30 years, 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 8 years from the notification point. After 30 years the data will be anonymised in line with article 5 of the of the General Data Protection Regulation (GDPR) and used only for clinical research studies.

Users are able to be deleted in line with their rights provided under the GDPR. We will action these requests when received and provide users 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.

If the services were no longer required or 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 health data retention policy as shown above.

The context of the processing.

This is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- The source of the data;
- The nature of your relationship with the individuals;
- How far individuals have control over their data;
- How far individuals are likely to expect the processing;
- Whether these individuals include children or other vulnerable people;
- Any previous experience of this type of processing;
- Any relevant advances in technology or security;
- Any current issues of public concern;
- In due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes;
- Whether you have considered and complied with relevant codes of practice.

Patient data is collected is directly from patients using the service. This is entered via an individual account controlled by log in credentials chosen by the user. This is currently single factor authentication with an email address and password. (aligning to my mhealth password policy). Clinicians are also able to add data such as observations and medicine changes following an appointment with the patient.

There are 3 separate relationships that form part of the service;
The relationship between the healthcare professionals

The Relationship between the procuring healthcare group and my mhealth. This provides the procurer access to a clinical dashboard to allow an overview of their patient care. For this relationship the CCG/TRUST is the DATA CONTROLLER for the CLINICIANS information within their clinical dashboard and my mhealth act as their data processor. There are contractual arrangements to manage this.

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.

The relationship between the end user (patient) and my mhealth. Once the patient accepts terms and conditions and privacy policy the direct relationship is formed with the user. my mhealth assume the role of the DATA CONTROLLER for the/any PATIENT DATA entered into the platform. The Clinicians 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 access to the platform is granted to that user.

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?***'**

The privacy policy also provides users with a transparent view of what their information is used for. Processing of their data is as expected for the service and does not include the processing of vulnerable individuals. myAsthma is available for patients from the age of 12 however, the terms and conditions and privacy policy need to be accepted by a parent/guardian/carer as they are under the age of explicit consent for the GDPR (age 13). All data is processed in line with the GDPR Requirements.

The purpose of the processing This is the reason why you want to process the personal data. This should include: • Your legitimate interests, where relevant; • The intended outcome for individuals; and The expected benefits for you or for society as a whole.
Processing the information collected is necessary to not only achieve the intended purpose of the service but also to achieve nationwide and legitimate objectives. The intent for commissioning the service is to provide a support tool allowing patients to feel empowered, to feel better educated, to better self-manage their diagnosed long-term condition(s) and support to healthcare professionals delivering their care. The innovation is to assist in managing the demand on the health services nationally by offering support to both parties. Clinicians are able to observe the patient's general ability to self-manage and to intervene where necessary remotely, when the patient is away from a clinical setting. This will not only see an increase in patient general reporting health and outcomes but will also reduce hospital admissions and present the health service with significant financial savings.

Consultation and Contacts

Please name the individuals (and their roles) that should be involved in this process. However, if you decide this is not appropriate, you should provide a clear explanation why.	**Head of Compliance**: David Hale 01202 299 583, david.hale@mymhealth.com **Data Protection Officer / Caldicott Guardian/ Medical Director**: Dr. Adam Kirk, 01202 299 583, adam.kirk@mymhealth.com **Senior Information Risk Owner (SIRO)**: Dr. Simon Bourne, phone 01202 299 583, simon.bourne@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. We also recommend you consider seeking legal advice or advice from other independent experts such as IT experts, sociologists or ethicists where	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 and Clinical Practices Locations where the service is being procured for (regions forming part of an STP for example)

appropriate. However, there are no specific requirements to do so.	

Assess necessity and general questions

Does the processing actually 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	For my mhealth this is **Consent, article 6 (1) a)** The activation link presents the patient with the terms and conditions and privacy policy that has to be an explicit opt in of consent. Health care providers or Trusts will be acting under article 6(1) (e).
What if Consent is not obtained	Any data could only be shared by legal enforcement. There wouldn't be any data to share at this stage though if there was no consent to process – consent is required for access to the service
Will reports be generated from this information. If yes, will the information be identifiable or anonymous (will the reports be used for research)	Yes. NHS administrative levels and my mhealth assigned project managers will be able to have reports on patient licence distribution. The trust/CCG are not able to access Patient personal data. These will be anonymised reports NHS clinician personal data may be accessed by higher administrative levels for facilitating contact. This is fine as the controller. Health Research Authority (HRA) approved research request will be looked at within specific information governance processes before data can be accessed and the patient would have given explicit consent at activation.

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 the clinician 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
How will data breaches be reported?	My mhealth Limited will alert the designated contact of a breach. This makes it important to communicate any updates to IG Lead or contacts, for us to be able to do this. Where applicable, my mhealth will file the breach at NHS / DSPT reporting tool and report to the ICO.
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, 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.
How easy would it be to migrate data from the cloud provider following termination of service?	The data will be available to be exported and given to the controller.

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 or write to support@mymhealth.com
Out of office hours: write 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.