Project Information;	
Project Name:	Deployment of the my mhealth self-management platform
Type of supply;	Web based software as a service (SaaS)
Data Controller for the project?	By purchasing our service, you the buyer, act as the Data Controller. My mhealth will become joint controller upon the patient licence activation, if you are an individual being provided the service by your healthcare team. As an organisation/region providing/procuring our service to be distributed via your geographical healthcare teams, in turn you will; • Decide which individuals to collect personal information about • Make decisions about the individuals concerned, from our processing of data • Have appointed us, by contract, to process the data on your behalf and; • Have a direct relationship with the data subject For more information please view our privacy notice at www.mymhealth.com/privacy.
Project Summary;	
myCOPD, myAsthma, myDiabetes, myHeart and myTelehealth are end-user applications developed by My mHealth Limited, to support patients to self-manage their condition, enabling clinicians to manage patient populations remotely and at scale. The apps are evidence-based interventions which have been through several rigorous evaluation processes including the NIA, SBRI, NHS England, and have been peer and user reviewed.	

Supplier Information;	
Name;	My mhealth Limited
Company No;	07881370
Address;	My mhealth Limited 1st & 2nd Floor 8 Trinity 161 Old Christchurch Road Bournemouth Dorset BH1 1JU
Telephone Number	01202 299 583
Web site	www.mymhealth.com
NHS Organisation Code	8JH30
ICO Registration Number	ZA151364

Compliance General;

Are my mhealth applications;	
NHS DSPT Compliant	Yes Level 2 compliance 89%
NHS App store approved	Yes NHS Digital, have conducted an extensive assessment on my mhealth products involving technical stability, clinical safety and regulatory aspects.
Medicine Health Regulatory Authority (MHRA) registered	Yes, as a class I medical device and can be viewed on the MHRA website under ref 6169
Bearing the CE Marking?	Yes, this can be viewed on our website at www.mymhealth.com
Compliance summary;	
Regular monitoring of Data Protection and Information Security takes place. Activity logs are maintained documenting IG initiatives, recommendations, incident management, data breaches, spot checks, staff induction and training. In line with my mhealth ongoing quality management system. This also includes a documented work plan covering management activities, meetings and reports delivered to/by the Board of Directors. My mhealth products are subject to external and internal information security assessments and monitoring, from which recommendations are reported and implemented.	

Service Implementation & Maintenance;	
Which web browsers are required/supported to run the app?	You can use a variety of browsers; Edge 13 or above; Chrome 43 or above; Chrome 53 for Android or above; Firefox 36 or above; Safari 9 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 additional browser plug-ins required?	No additional browser plug-ins i.e Flash or Java are required.
Where can I view the my mhealth 'terms and conditions"	Our "Terms and Conditions" can be viewed at https://mymhealth.com/terms
Where can I locate your service Level Agreement (SLA)	The SLA is the final pages of this document
Are there any additional technical requirements?	
For access to the service as an individual you will need either to: a) Download the my mhealth app from Play Store or Apple Store or; b) use their preferred web browser(s), outlined above. If you are a Healthcare professional, you may need your 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.	
What training & support do you offer for implementing the service	Training and ongoing support can be offered. If you are an organisation region/health board providing the service this will depend on your individual bespoke agreement. If you are an individual, you can view the "how to use" tile within the app or contact our support line on 01202 299 853 If you are a clinician requiring technical support, you can also contact our support team on the above number.

Collecting, Sharing & Protecting your information;	
What information will be collected?	We will only collect the information necessary to deliver our service(s); If you are an individual this will consist of, but not limit to, sensitive information such as, your basic contact details, symptoms, nutritional data, medication adherence, location (GPS and/or postcode), disease details and metrics, analytical data including video usage, login details, and device information. If you are a representative of an organisation/healthcare professional we will collect your name, role, email address, telephone number, organisation or team name.
Why is my information being collected?	To support patient with self-management and education of long-term conditions, support clinical management of local patient populations and to manage the distribution of software licences to patients.
How will you collect information?	We will collect information that is entered by either the user of the app or the clinician involved with their direct care.
Where will my data be stored?	We store your data In Amazon AWS (London availability zones only). There are no data transmission across UK boundaries. Their infrastructure is a server cluster providing data redundancy and network isolation / security. Also providing high availability (3x) with redundant network connectivity and power supply.

Can my information be viewed, edited or deleted	Information that is entered into the app by an individual or healthcare professional, such as, but not limited to medications, targets, readings and symptoms scoring can be edited, viewed or deleted within the app. Data subjects can also exercise their rights in line with the GDPR by contacting us.
Will you record my access to the app?	Yes, we will record your log in frequency and activity to ensure the effectiveness of the app
How will my information be quality checked?	Information within the app will be quality checked manually as part of regular consultations between clinicians and the patient. The patient will also be able to quality check their own information, in line with the intended purpose of a self-management platform.
How will consent be obtained to process information?	Consent is given by a public Privacy Policy accepted by each patient before entering the platform. Privacy preferences can be updated at any point within the “My Account” tile.
If consent is not obtained, will you still share identifiable information?	Only by legal enforcement, such as a court order
Who is information shared with?	The Patient data will be shared with clinical team(s) providing direct care. Access to clinicians is granted and revoked by a clinical manager role and by the patient. CCGs and other higher administrative levels will only access anonymised data or corporate data, including details of sub-managers or clinicians involved in the project. So; Patients: access their own data only; Clinicians: access data of patients under direct care only; Clinical managers: access anonymised data and their clinicians contact details; Administrator roles: access patient anonymised data and their sub-user corporate contact details; System administrators (my mhealth): access the underlying system as a data processor under contractual clauses and additional security measures.
How long will you hold information for?	We will hold information that has been collected by entry from the user or clinician for 30 years and/or for a period of 8 years if the patient is

	deceased, in line with NHS Chronic conditions data retention guidance. To adhere to these guidelines we require notification, should a patient be deceased
For full details on why, how and where we collect, share and process your data please view our privacy notice at www.mymhealth.com/privacy	
Will you let me know if you make changes to your privacy policy?	Any changes to our privacy policy will be done so, in collaboration with any joint data controllers, then published on the my mhealth website and finally, a notification to individual users via the app.
What happens in the event of a data breach?	We will contact the individual and /or CCG IG Lead or other designated NHS contact, dependant on who we have been provided. A breach by Mymealth will be dealt with in line with the ICO guidance and advise the joint controller of the incident and resolution. Where applicable, my mhealth will also file the breach at NHS / DSPT reporting tool.

Security & Due Diligence;	
Do you carry out due diligence on new employees/contractors?	All employees are subject to DBS checks. Any Contractors are to sign a data sharing agreement stating that any transmission and use of the data is forbidden and only system operations are allowed.
Are the my mhealth system(s) protected from Viruses and any malicious codes?	Yes, we enforce a robust quality management system of which, these areas form part. Examples of this but not limited to would be; filter of all incoming and outgoing data, virus scanning of all tools involved within the software build, this is Cisco ClamAV (an anti-virus tool kit) prior to implementation and regular reviews of the physical premises.
Are there anti- virus solutions/software in place to scan for malicious code?	Yes
What are the security measures in place for my mhealth employees to ensure patient confidentiality?	Employees with access to patient data are those where it is necessary and is limited to named, designated full-time employees holding contract confidentiality clauses and utilising AES-256

	encrypted, multi-factor authentication access. This is also monitored on a daily basis. Employees need to comply with company policies, covering both the work environment in Bournemouth and when working remotely. Examples of this would be; physical access control, mobile-work acceptable use of devices, and the delivery of sensitive access details.
What user authentication methods are offered?	Multi-factor authentication methods are in place. The user requires a username and password to use and access the service. There is a minimum level of password requirements built into the app and has to be met when setting up the account. If the user is 'locked out' following 3 failed attempts, they will need to reset the password.
How will information be transported? i.e Data in transit	Information will be transported via network only with Transport Layer Security **(TLS2.1),** which is a cryptographic protocol used to increase security over computer networks, and **AES-256 (ciphers),** a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files.
Do we comply with OWASP security standards?	Yes, we also follow OWASP developer's guidance and the OWASP tools for data filtering. Our external security assessments ("pentesting") are based on OWASP and any auditor recommendations are reviewed and implemented, where applicable.
What security measures are in place?	Procedures are documented, distributed and maintained for: data handling/ management, operating procedures and physical access to the building. **Please see below for specific areas;**

For a description of "Data in transit" please see the data transport section above.

Ciphers (AES-256) 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_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Information stored is encrypted (AES 256). Firewall, NAT, Security Groups, namespace segregation and systems configuration implement a 'allow only enough' principle (least privilege).

Systems security patching, internal and external security audits, software quality assurance process and application security updates are all part of the software

development lifecycle, as well as, policies on network configuration, security advisory reviews covering full stack software components, and IT staff training on security.

Physical security
Keyholders are logged and passwords are stored in audited, compliant encrypted vaults and follow a strict Password Policy. There is CCTV in operation 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, a pseudorandom function and all incoming data is filtered using OWASP sanitisation. HTML (a mark-up language to create a web page) and application code are disallowed as content in the database, data caching is disabled in web browsers and any notification/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.

What sharing agreements will be in place?	All commercial relationships will be bound by a contract and where applicable, data sharing agreements. Direct user relationships will be bound by the privacy notice. All employees of my mhealth also have a contract in place.
What reports will be generated from the information collected?	NHS administrative levels and my mhealth assigned project managers will be able to have reports on patient licence distribution. Patient personal data will not be accessed in any case. NHS clinician personal data may be accessed by higher administrative levels for facilitating contact. Other reports are not part of the current scope. Future research initiatives will be subject to specific ethics approval and specific information governance processes (patient consent, etc.) before data can be accessed.

Risk, issues & activities;	
Please request/refer to the my mhealth DPIA (Data Privacy Impact Assessment) in which risks and their prevention are detailed.	
Are there any known risks directly affecting the service?	Network administrators in local facilities will probably need to grant access to the mymhealth.com domain and to the Vimeo content delivery network. Not using the latest

	Web browsers would reduce the level of innate security offered by the most recent versions.

Cloud Environment;	
Is Amazon Web Solutions based on public, community or private cloud(s)	Public cloud. Please refer to the storage section of Protecting your information, within this FAQ for more information.
Where will the information be physically located?	Information will be held in the UK and occasionally, may be stored within the European Union.
How can I contact AWS?	Amazon UK Services Ltd. Patriot Court 1-9 The Grove Slough, SL1 1QP United Kingdom Tel. 08004961081
Are servers shared with other AWS users/customers?	No, servers are segregated for each AWS user i.e. my mhealth have their own server.
Does AWS hold security related certificates for their service?	Yes, AWS are aligned with the G-Cloud and hold the following certifications / attestations: ISO/IEC 27001, PCI DSS Level 1, HIPAA, Cyber Essentials Plus UK, ISO/IEC 27017 and others. AWS UK hold Public Services Network (PSN) assurance, which provides UK Public Sector customers with an assured infrastructure on which to build UK Public Sector services.
Do AWS meet Tier-X standards?	Amazon Web Services London are made up of a cluster of Tier-4 connected data centres.
Will information be able to be migrated in the event of my mhealth termination of service or insolvency?	Information would be available in a format to be exported by the Data Controller
Can information within AWS be accessed?	Yes, as the app works as a user interface the information viewed by the user is being viewed within AWS.
Can information availability be guaranteed?	AWS information is stored in 3 separate physical locations to provide power supply and network connectivity segregation/redundancy. At database level: data replication in 3 physical servers in a master less, distributed database system. At application level: redundant / load-balanced app stateless web services. At Disaster Recovery level: daily data backup to AWS S3

How do AWS remove information from its devices following termination of service?	AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of their decommissioning process.”). This can take up to a period of 6 months to fully complete.

Service Level Agreement (SLA)

Version 1.3 – 21 March 2018

My mHealth Service Level Agreement (SLA) is a policy governing the availability and IT support of the systems, networks, storage and application services provided by My mHealth ("We") and its affiliates to their customers ("You").

Service constraints

In order to access the Service, you will be required to have:

(a) A stable Internet connection and unrestricted access to Internet resources required by the Service;

(b) A reasonably updated web browser. Currently My mHealth officially supports the following browsers and versions: Internet Explorer 11; Edge 13 or above; Chrome 43 or above; Chrome 53 for Android or above; Firefox 36 or above; Safari 9 or above. Updates to this list may be made in the future in particular to address security vulnerabilities.

Network Service

Reasonable commercial efforts will be used to provide a 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 attached storage volumes perform zero read-write IO, with pending IO in the queue.

IT Service Support

The service will be monitored by our IT staff 24 hours per day, 7 days per week.

A team of IT developers/operators will be available during common weekday office hours matching the region where the service is deployed subject to the Statement of Work (SoW) or equivalent contractual arrangement.

In the UK, this is from 08:00 until 17:00 UTC±00:00 from Monday to Friday except Bank Holidays. For other regions, equivalent arrangements will be made under the Statement of Work (SoW) or equivalent contractual arrangement.

During out-of-office hours, including nights, weekends and public holidays, a designated IT member of staff will be on call. Depending on the evaluated severity of the event, additional IT human resources may be in place to mitigate a reported incident.

IT support contacts in the UK are:

Office hours: call +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 2 hours during office hours and 8 hours during out-of-office hours.

Changes to the IT service

If the commercial relationship between us and you is based on an agreed Statement Of Work (SoW) detailing development and maintenance of systems or applications, any relevant change on systems, network architecture, hosting service, software functionality and IT service will be proposed to you detailing changes and timings.

By "relevant changes" we mean:

a) system or network configurations that affect the network or system architecture previously agreed in the SoW.

b) software releases that change functionality specified in the SoW.

c) IT support services.

Changes will be requested to a designated contact in your organisation (an individual or department responsible for project management). Your organisation is responsible for keeping us updated on the designated contact.

Incident reporting

My mHealth will notify you of any relevant incident affecting the service, including service unavailability, functionality disruption, data loss or systems hacking.

Although systems are designed for 24x7 availability, my mHealth will also inform you of planned maintenance activities that potentially may disrupt the service.

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

In rare cases when regular maintenance notifications are required for all users, namely a) legal pre-notification of an update to the Privacy Policy, b) planned technical maintenance activities affecting the service and c) information about unexpected service disruption, we will directly notify users via the notifications functionality in the app.

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 arrangements.

Planned Maintenance Periods

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

Data Retention

During the service, an Information Governance officer will be available to reply to any queries, manage the data retention policy and manage the initiation of record destruction.

Personal data will be kept for a period of time and then destroyed. Retention periods are agreed in the service contract, or otherwise follow my mhealth's Data Retention Policy. Data may be deleted prior to these periods for reasons of law enforcement or a request of deletion by the data subject after identity validation.

A log of destructed records will be kept, including a data subject identifier, the type of data destroyed, the time that the data refers to, and the time of deletion.

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 an agreed SoW (Statement of Work) or other commercial arrangements may or may not override or complement this policy.