

# Data Privacy Impact Assessment (DPIA)

## Part 3: Full Data Protection Impact Assessment (DPIA)

<b>DPIA Ref (for CDPU use only)</b>	
Process/Project Name:	MyMHealth
Project Lead:	[name redacted]
Project Manager (where applicable):	[name redacted]
Person completing form (If different to above)	[name redacted] [job title redacted]
Date on which processing will commence:	TBC

<b>Part 3: Full Data Protection Impact Assessment (DPIA)</b>
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.
<b>Section 1 – Necessity and Proportionality</b>
In this section you must demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment. <ul style="list-style-type: none"> <li>The processing must be <b>necessary</b> for the specific objective of the process/project/proposal.</li> <li>It must also be <b>proportionate</b>, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.</li> </ul>
<b>1.1 What do you want to achieve from the process/project and how will your plans for processing personal data help to achieve your purpose?</b> <ul style="list-style-type: none"> <li>Clearly state your objective</li> <li>Provide evidence for why the proposal is necessary. The evidence can consist of facts, statistics, reports etc.</li> </ul>
<p>MyMHealth is a digital solution for long-term condition management, specifically Asthma, COPD, Diabetes and Heart Disease. HCS have considered this system for some time, but arrangement for the Covid-19 response has accelerated the implementation as we are unable to offer clinics, but need to maintain the monitoring of our patients with long term, chronic conditions remotely.</p> <p>The initial implementation (Phase 1) will be limited to COPD patients (c800) and Heart patients (c600).</p> <p><b>myCOPD</b> myCOPD is for patients suffering with Chronic Obstructive Pulmonary Disease. The evidence from 3 clinical trials illustrates</p> <ul style="list-style-type: none"> <li>Corrects 98% of the inhaler errors present in 90% of patients</li> <li>Delivers pulmonary rehabilitation with the same outcomes as classed-based programs</li> <li>Reduces readmissions</li> <li>Speeds the recovery from acute exacerbations</li> </ul> <p>Functions</p> <ul style="list-style-type: none"> <li>Symptom tracking via CAT scores</li> <li>Self-management</li> <li>Medication Diary</li> <li>Pulmonary rehabilitation</li> </ul>

- Inhaler, nebuliser and spacer videos for every device
- Smoking cessation
- Comprehensive education course
- Chest Clearance
- Weather and pollution forecasting

### **myDiabetes**

Our QISMET approved app is for patients suffering with Type 1 or Type 2 Diabetes, including those controlled with diet, tablets and/or insulin. The App intelligently populates its content in order to customise the education and interventions delivered so they are relevant for the different patient groups.

myDiabetes brings patients the most comprehensive self-management diabetes app available on any device. Built by clinical experts, with patients, myDiabetes puts individuals in control like never before. myDiabetes contains expert education on all aspects of diabetes care and allows them to monitor their blood glucose, HbA1C and other risk factors to reduce their risk of serious long term complications.

Functions

- Medication Diary
- Diabetes Checklist
- Targets and goal setting
- Risk factor management
- Comprehensive reports
- Complete diabetes course
- DMFit - Type 2 diabetes intervention program

### **myAsthma**

myAsthma empowers patients to manage their asthma for a lifetime. Based on best evidence and national guidelines, myAsthma provides 24-hour self-management, expert advice and support for patients with adult asthma.

myAsthma is the first of our apps with my mhealth AI which analyses patients' symptoms, and medication use, to facilitate health using our unique algorithms. It was also our first product to deliver the automated annual review, which reduces the time for this to be delivered in primary care by 75%.

Main Functions

- Asthma Action Plan
- Online Medication Diary
- Symptom tracking via ACT
- Online Peak Flow diary
- Inhaler, nebuliser and spacer videos
- Prescription assessment
- Hay Fever Score
- Weather, Pollen and Pollution forecasting
- Comprehensive

### **myHeart**

myHeart is a comprehensive platform for patients suffering with heart disease, and for those who have undergone recent heart surgery.

The App delivers an individualised self-management and cardiac rehabilitation platform that is customised to the individual. Using our award-winning rehabilitation platform, and integrating over 50 new Education videos, myHeart brings the very best support to patients suffering with these conditions. Like all our applications, myHeart comes complete with a clinician interface enabling remote care, at scale to this population.

Conditions covered:

- Heart Failure
- Angina
- Heart Attack
- Post PCI
- Valve Replacement
- Valve Repair
- Coronary Artery Bypass Graft Surgery
- Valvular Heart Disease

#### Key Features

- Full cardiac rehab program relevant to the condition
- Post-surgery recovery program
- Lifestyle and risk factor interventions
- Store and view ECG and ECHO reports
- Comprehensive individualised patient education course
- Post-surgery and post-heart attack educational course

#### CLINICAL INTERFACE

This will enable us to manage and support the patient population at scale, using up to date, co-scripted data. Well, this is now possible using the myhealth clinical dashboard. Let's start with the patient list.

##### Patient list

The patient list, is where clinicians manage, search and organise their patients. It is dynamic, allowing clinicians to order patients according to symptoms, QOL (Quality of life), or severity. For example, you can prioritise patients with COPD or Asthma, according to their exacerbations status, or for patients with Diabetes you can find out instantly who needs their annual eye check, and when, or order patients with the highest HbA1C. Each condition, has an optimised patient list with all this functionality integrated. For example, if you are running a pulmonary, or cardiac rehabilitation course remotely, you can find out which patients are exercising, and how far they are through the education program; enabling clinicians to be active in the rehabilitation of hundreds of patients, many of whom find access to face to face rehabilitation difficult.

##### Notifications

From the patient list you can send a message to an entire, disease specific, patient population, for example send a message to your asthma patients that the flu vaccine is now available.

##### Map function

For patients with COPD it might be important for you to review visually the exacerbation burden in your community, or to assist the prioritisation of visits from community clinicians. You can do this using the map function.

#### 1.2 Describe why existing and/or less intrusive measures would be inadequate

- Describe whether any less intrusive options would achieve the same goal.
- Consider whether existing processes or techniques could be used instead of new intrusive measures
- Clearly outline why the processing is proportionate

The cancellation of clinics and out-patients appointments to support and enable HCS' response to the Covid-19 pandemic has highlighted a requirement for the remote management of patients in the Island. Clinicians having access to the data through the interface will allow the continued management of patients and efficient and effective (and safe) care delivery. The use of the app will not mean a detrimental impact on the level care experienced by those that are either unable or unwilling to consent to such a service. Use of the app will be in addition to the 'regular' service offered.

#### 1.3 What is your intended effect of the processing to the SoJ, the Data Subjects and/or Society and the general public

- Describe benefits or disadvantages to the above

##### Benefits:

- Clinicians can monitor the health of their patients without risking exposure to Covid-19 via hospital appointments
- Those in scope of the app are considered high-risk individuals and exposure to Covid-19 could have a significant impact on their health
- Location data will help the outreach teams manage their programme, and transport equipment / oxygen efficiently whilst short of resources
- Patients will know that they continue to be monitored and under our care
- Patients have access to resources that can help them to live with their condition, including exercises that can be carried out whilst self-isolating
- Clinicians can set targets and access current data relating to their condition and their symptoms
- Self-management plans can be clearly articulated and accessible to both patients and clinicians

There is no requirement for patients to use this App – it will be offered as an adjunct rather than an either/or and it will not affect their current standard of care. Patients will be advised that they can on-board / off-board as they wish.

Testing the app, and the clinical interface has been beneficial to ensure that the app is the most appropriate for our jurisdiction, that it is easy to use for a range of users and for those with differing levels of technical ability. Special care should be taken to ensure that we can offer the app to those with differing needs and disabilities.

## Section 2 – Scope

### 2.1 Provide full details of the specific personal data that you intend to process

- Any information that the patient puts into the system. This can include name, address, email and NHS number / URN.
- MyMHealth may collect additional information from your device, such as, data provided by sensors like location and acceleration, by applications like web browsers, the devices' IP address and the time and duration of any activity.
- It will record patient app usage to understand how the service is used and which sections are used most and to review progress through the courses available on the app(s).
- Information put into the system by the HCS healthcare team in working with the patient and their condition.
- Geolocation.
- Information from third parties that form part of our services, such as pollen feeds, pollution feeds and localised weather information (geo-located to your whereabouts).

### 2.2 Describe the volume and variety of personal data you intend to process

See section 1 and section 2.1

### 2.3 How long do you expect the processing to last?

For the duration of time that the patient is in the care of the clinician, or until the patient chooses to stop using it at which point they can request their data be deleted by the supplier.

### 2.4 Have you considered any approved codes of conduct or certification schemes?

If Yes please provide details in the text box.

- Yes  
 No

The NHS have approved this app for use across the NHS, and it is available in the NHS App Store.

### 2.5 Special category data – Will you be processing any of the following special categories of data?

- |                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Race<br><input type="checkbox"/> Ethnic origin<br><input type="checkbox"/> Political opinions<br><input type="checkbox"/> Religion<br><input type="checkbox"/> Philosophical beliefs<br><input type="checkbox"/> Trade union membership | <input type="checkbox"/> Genetic data<br><input checked="" type="checkbox"/> Biometric data<br><input type="checkbox"/> Sex life<br><input checked="" type="checkbox"/> Health<br><input type="checkbox"/> Criminal record<br><input type="checkbox"/> Alleged criminal activity |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 2.6 Please specify the applicable legal basis or enactment for processing this data

(Informed and Explicit) Consent  
 Users must be made fully aware of how their data is processed and their rights.  
 The app should not be used for anyone under the age of 14.  
 Special care must be taken to ensure the capacity to consent.

### 2.7 Please indicate the appropriate processing condition(s) below

**General data processing**

- Consent
- Legal obligation
- Employment and social fields
- Vital interests
- Legal proceedings
- Public functions
- Public interest
- Medical purposes
- Public health
- Archiving and research
- Avoidance of discrimination
- Prevention of unlawful acts
- Protection against malpractice and mismanagement
- Counselling
- Functions of a police officer
- Other (please specify below)

**Section 3 – Consultation**

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.

**3.1 Do you intend to consult data subjects?**

**Yes**

If yes then outline your plan in **Section 3.2** below together with details of consultation with other stakeholders.

**No**

If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 3.2** below.

Data subjects are consenting to the use of this service / app, and HCS will work with the supplier to ensure that patients are fully informed of how their data is used and processed prior to their on-boarding. There is no requirement for patients to use this service, and no detrimental effect on their care if they choose not to participate.

**3.2 Consultation Action Log**

**Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:**

Who	When	How	Outcome
[Name redacted]	04/05/2020	Email DPIA	Response regarding technical platforms and plans for integration
Andrew Mitchell	08/05/2020	Email DPIA	
[name redacted]	04/05/2020	Email DPIA	Supporting information relating to integration plans and the technical platforms
John McInerney	04/05/2020	Email DPIA	Queries relating to territory, retention schedules and the use of data for secondary purposes. Raised issue of access for those with physical needs or no access to the platform.

			Keen to ensure that the consent is fully informed and explicit. This will be addressed by the on-boarding process
[name redacted]	04/05/2020	Email DPIA	
[name redacted]	08/05/2020	Email DPIA	

**Section 4 – Information Lifecycle**

**4.1 Provide a full description of the information lifecycle**

<b>Stage of Processing</b>	<b>Description</b>
<p><b>Collection</b> Where does the data originate from, who will collect it and how will it be data obtained?</p>	<p>The data originates from the patient, who sets up an account and is linked to their HCS clinicians through the clinical interface. Relevant data is inputted by both the patient and the HCS clinician.</p>
<p><b>Storage</b> Describe where and how the data is to be stored</p>	<p>MyMHealth Data and information is stored within cloud-based servers situated within the EEA. All information kept by my mhealth is encrypted when it is being moved between devices but also when it is stored using the industry standard. mHealth have strict procedures and security measures to prevent unauthorised access or disclosure of your information and are accredited by Cyber Essentials + .</p> <p>HCS will access the information using Government of Jersey devices and networks, and the clinical interface will store the information in the cloud. Access to the data will be limited to those requiring administration access (HCS Digital Health) and for support purposes.</p> <p>There are no plans to integrate the data held in myhealth with any other system.</p>
<p><b>Use</b> Describe how the data will be used. Describe whether it involves new technology or novel processing.</p>	<p>MyMHealth will use data in the following ways:</p> <ol style="list-style-type: none"> <li>1. To provide the service To register and manage the account and to ensure information is accurate and up-to-date To enable users to work together in a safe, secure environment To inform alterations, modification, updates and improvements in the service To review, investigate and address issues that may affect use of the service</li> <li>2. To exercise the supplier’s legitimate interests MyMHealth will use data to review and assess the quality of the service and make improvements They need to use the information to provide a responsive service and be able to support or respond to your contacts They will use information for internal operations. These might</li> </ol>

	<p>include troubleshooting, fraud detection and resolution, data quality checks, functional testing, security, audit and statistical analysis of the app/service</p> <p>3. To respond to obligatory requirements</p> <p>MyMHealth will disclose information if they are requested to do so as part of a reasonable regulatory requirement or in response to a legal request.</p> <p>HCS will use the data in the following ways:</p> <ul style="list-style-type: none"> <li>▪ Clinicians can monitor the health of their patients without risking exposure to Covid-19 via hospital appointments</li> <li>▪ Those in scope of the app are considered high-risk individuals and exposure to Covid-19 could have a significant impact on their health</li> <li>▪ Location data will help the outreach teams manage their programme, and transport equipment / oxygen efficiently whilst short of resources</li> <li>▪ Patients will know that they continue to be monitored and under our care</li> <li>▪ Patients have access to resources that can help them to live with their condition, including exercises that can be carried out whilst self-isolating</li> <li>▪ Clinicians can set targets and access current data relating to their condition and their symptoms</li> <li>▪ Self-management plans can be clearly articulated and accessible to both patients and clinicians</li> </ul> <p>NOTE – No data will be used, by HCS or MyMHealth will be used or sold for marketing purposes.</p>
<p><b>Access</b> Describe who has access to the data throughout the life of the processing</p>	<p>MyMhealth will have access to the data, held in cloud based servers in order to manage the account, make improvements, troubleshooting, fraud detection and resolution, data quality checks, functional testing and analysis.</p> <p>Within HCS, access to the data will be limited to those that 'need to know', i.e. they are responsible for managing the service and administering the care of the patients. Role based access will be monitored regularly. Support and administration will be conducted by the supplier, and Digital Health.</p> <p>Access to HCS Information Governance for the purpose of complying with disclosure requests such as SARs or police requests will be via Digital Health support team. Any disclosures will be conducted in line with our statutory obligations.</p> <p>Access to the data for any other purpose, such as SI and complaint investigations will be via the Digital Health support team.</p>
<p><b>Recording</b> Describe the processes for recording the data</p>	<p>Data is recorded by both the patient and the clinician. It allows the recording of stats / functions and blood pressure for example. It also allows for messaging between clinician and patient.</p>

<p><b>Processors</b></p> <p>Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the EU?</p>	<p>Data will not be processed outside the EEA.</p> <p>There is a contract in place to regulate the relationship and the Information Asset Owner is [name redacted]. The contract will be reviewed after 1 year.</p>
<p><b>Sharing</b></p> <ul style="list-style-type: none"> <li>• With which external organisation(s) is the data shared, what data is shared, and why?</li> <li>• Describe any sharing that will occur within the SoJ</li> <li>• Outline any national and international sharing or processing.</li> </ul>	<p>MyMHealth will use the information to support patients, for them to record your symptoms, learn more about their condition and as a result, improve self-management. To do this, we may share information and anonymised information, depending on the service, with third parties such as;</p> <ul style="list-style-type: none"> <li>▪ Information storage providers</li> <li>▪ Push notification software providers</li> <li>▪ Healthcare &amp; research teams</li> <li>▪ SMS messaging services</li> </ul> <p>MyMHealth will only share the minimal information necessary to deliver the service.</p> <p>As a medical company, MyMHealth take part, where approved by the relevant authorities, in assisting with studies and medical research. This is to help understand more about the condition and the improvement of future treatments available to patients with the condition. To do this MyMHealth may contact users when these types of opportunities arise. MyMHealth will ensure that patients can consent to this type of activity before any further information processing takes place. HCS should pay special attention to any unintended consequences of the use of anonymized patient data for research. Where HCS are asked to provide data of our patients for use in research, both the consent of the patient and ethics committee approval should be sought.</p> <p>HCS will share information without consent only where there is a statutory obligation to do so. Any requests for sharing should be referred to Information Governance and the Caldicott Guardian.</p> <p>Otherwise, any sharing of the data outside of HCS, for overseas treatment, for example, will be on the legal basis of consent.</p> <p>Whilst there are no current integration points, there are future plans to integrate with EMIS and the Acute EPR. Plans should be fully assessed for privacy and unintended consequence prior to any integration with other systems and any sharing with GP surgeries will be agreed by the Health and Care Information Sharing Board.</p>



<p><b>Review and Retention</b></p> <p>Describe your plan for review and retention, linking to a retention schedule where appropriate</p>	<p>MyMHealth will keep the information for up to 30 years, unless the user is still actively using the platform. The app is for those with long-term conditions and potentially the record if live, and still in use, may be maintained for longer. If the patient instructs MyMHealth to stop processing their data then this will be actioned and data will not be held for this period. If MyMHealth are notified by the healthcare professional that the patient is deceased, they will then store their data for 8 years, again in line with medical regulations. The data is not anonymised nor is it shared.</p> <p>If asked to delete your information before this, MyMHealth will, but it may take up to 6 months to completely remove the data from the cloud-based back-up storage system. Following the death of a user, these rules will apply unless MyMHealth are informed directly.</p> <p>HCS will retain data in line with their retention schedules.</p>
<p><b>Disposal</b></p> <p>Describe the process for disposal of data, including when and how.</p>	<p>MyMHealth</p> <p>MyMHealth will delete data held on request of the user but advise that it may take 6 months to remove completely from the cloud based back-up storage system. If a user requests for MyMHealth to stop processing or simply stops using the app then it needs to run a period with AWS within a non-used data repository, after this period of non-activity the information will then simply 'drop off'.</p> <p>Data held by HCS will be disposed of as per our usual process.</p>
<p><b>4.2 Diagrams and Tables</b></p>	
<p><b>4.3 Assets</b></p>	
<p><b>Asset</b></p>	<p><b>Description</b></p>
<p><b>Hardware</b></p>	<p>Patients will use their own devices which require an Internet connection. They are able to use laptops, phones. Clinicians will use their own devices (as per BYOD policy) or GoJ networked devices for access to the data, as will the Digital Health support team.</p> <p>Devices required for data input include scales and fitness trackers. They are Bluetooth enabled and device agnostic.</p>
<p><b>Software</b></p>	<p>MHealth Suite and AWS SaaS</p>
<p><b>Networks</b></p>	<p>Jersey Telecom, patient's own network and GoJ network</p>
<p><b>Hardcopy/paper</b></p>	<p>Not applicable</p>
<p><b>Any other relevant assets</b></p>	<p>Not applicable</p>

## Section 5 – Full Risk Assessment

### 5.1 Fair, Lawful and Transparent

Data must be processed lawfully, fairly and in a transparent manner

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Service Users are unaware of what we are processing relating to them or what we use it for, including who we share it with	Reasonable / Possible	Some Impact		On-boarding pack to be produced that outlines the system, how it is used, who has access to the data and how we will keep it safe. This is to be made available prior to the patient agreeing to its use so that consent is explicit and informed.	REDUCED	
The HCS Privacy Notice does not reflect this sort of processing or sharing and service users are unaware that their data is being shared in this way.	Remote	Minimal Impact		Information Governance to review HCS privacy notice and assure that it covers relevant processing for this group.  MyMHealth Privacy Policy to be made available to all patients in scope prior to them on-boarding	REDUCED	

[Type here]

### 5.2 Specific, explicit and legitimate purpose

The purpose for which you process personal data must be specified, explicit and legitimate. Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
<p>The data collected that relates to the service user is used for purposes other than what it was collected for</p> <p>Most users will consider their data private to HCS and MyMHealth and would not expect that we share to other agencies</p>	Reasonable / Possible	Some Impact		<p>Contractual assurance that data is used by MyMHealth for a secondary purpose only with the consent of the patient.</p> <p>Reporting of any breaches or incidents will be done through Datix, and pseudonymised where possible. Access to Datix will be limited to those that need to know.</p> <p>Requests for the data held in the clinical interface from the police or other third parties will be referred to IG who will consider the public interest in sharing the data, and apply best practice guidelines.</p> <p>Data shared under a specific statutory obligation will be logged, and where appropriate, the patient will be informed.</p>	REDUCED	

[Type here]

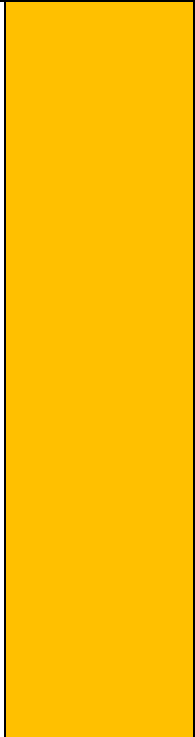
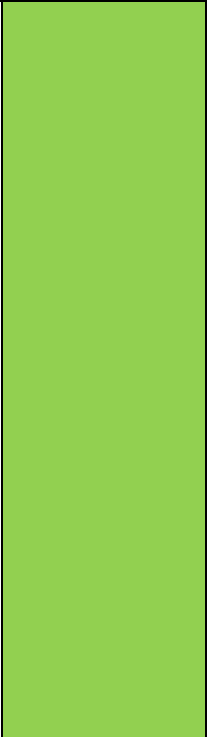
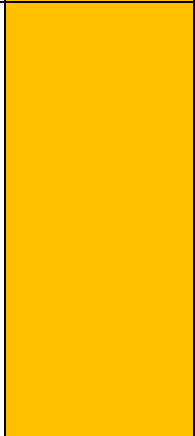
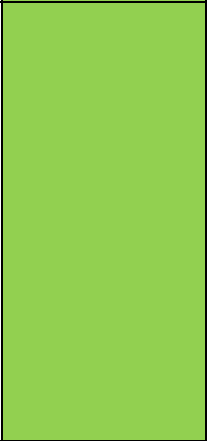
				<p>Any other secondary use by HCS will be based on informed and explicit consent.</p> <p>Aggregated data will be anonymized and may be shared within HCS for management reporting and clinical oversight, such as MDTs.</p> <p>Any use of the data for research purposes will be carried out only after a full DPIA is carried out and the ethics committee have approved.</p>		
--	--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

**5.3 Adequate, relevant and not excessive**

Personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
--------------------------------------------------------------------------------	--------------------	------------------	--------------	----------------------	--------	---------------

[Type here]

<p>Clinicians can access more information about service users than they 'need to know'</p>	<p>Reasonable / Possible</p>	<p>Some Impact</p>		<p>The Apps are designed to record and report information that is required in order to effectively manage the conditions as described in section 1. This will be monitored regularly and any issues with excessive data collection fed back to the supplier. Any patient misusing the system or adding data that is not required i.e. inappropriate messaging to a clinician, for example, will be managed appropriately, and any data relevant to other areas will be shared with the relevant clinician where consent has been given.</p>	<p>REDUCED</p>	
<p>There is little clarity provided by the supplier on the use of location data. Is it tracking all the time or when the app is in use – for what purpose does the tracking serve and, can the app be used without location data being enabled?</p>	<p>Reasonable / Possible</p>	<p>Some impact</p>		<p>Confirmation received from the supplier that the location data is not a mandatory requirement for use of the App. All patients can turn off their location data facility on their device, and the choice remains with them. The location element is only linked to the live feeds re pollen count / weather etc. these live feeds are limited only to things</p>	<p>REDUCED</p>	

[Type here]

				that may have an effect on the long term conditions in scope of MyMHealth.		
--	--	--	--	----------------------------------------------------------------------------	--	--

**5.4 Accurate & timely**

Personal data processed must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Data input by the patient is not available to the clinician due to system downtime / issues with access / network issues / security breach and clinicians are unaware that a patient is high-risk and needs care	Probable	Serious Harm		<p>There is continued work to improve the resilience and the security of the GoJ system.</p> <p>HCS to develop a business continuity plan that will detail the protocol to be adopted if the data provided to the clinical interface for any length of time. This will be complimented by the support contract and service level agreement to ensure that any downtime is prioritized in line with the clinical requirement and that there is no significant impact on the patient and their care.</p>	REDUCED	

[Type here]

**5.5 Retention**

Personal data must be kept for no longer than is necessary for the purpose for which it is processed.

Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Supplier does not manage their records according to retention schedules or their privacy policy	Reasonable / Probable	Minimal Impact		Information Governance to carry out due diligence and liaise with suppliers where retention schedules need to be applied.	REDUCED	
There is no clear process for the deletion of network data / data stored in L drives and no access to overarching systems like Varonis for HCS staff and so retention schedules are not and cannot be applied	Probable	Some Impact		ACTION: Process and Access to be relayed to HCS in order that they can comply – Long term requirement – MyMHealth project not dependent on this being fixed.	RESIDUAL RISK REMAINS	

**5.6 Security**

Personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
--------------------------------------------------------------------------------	--------------------	------------------	--------------	----------------------	--------	---------------

[Type here]

<p>Information is sent to other suppliers / healthcare providers and shared with organisations inappropriately</p>	<p>Reasonable / Probable</p>	<p>Serious Harm</p>		<p>Clarity on the need to know principle agreed through the Contract and scheduled procedures</p> <p>Named responsible officers to be agreed.</p> <p>Access to clinical interface to be tightly controlled and reviewed regularly</p> <p>ACTION: AG On-boarding and RBACs defined and process implemented</p>	<p>REDUCED</p>	
<p>There is no clear process for managing lost devices or devices that have compromised security</p>	<p>Reasonable / Probable</p>	<p>Minimal Impact</p>		<p>ACTION: AG On and Off Boarding process to be developed, along with information to provide to users re technical support and information security</p>	<p>REDUCED</p>	
<p>Information is not disposed of securely</p>	<p>Remote</p>	<p>Minimal Impact</p>		<p>Information Governance to carry out due diligence and liaise with suppliers where confidential disposal needs to be assured</p>	<p>REDUCED</p>	

[Type here]



The supplier has not gained the Cyber Essentials and Cyber Essentials Plus certification	Confirmed Risk	Serious Harm – potential risk to the GoJ infrastructure and information security requirements		MyMHealth have recognized the need for accreditation and having made some remedial improvements, have been accredited by CE+. No further action required	REDUCED	
It is not clear who has responsibility for the management of data breaches	Reasonable / Probable	Serious Harm		Supplier and Project Manager / Information Asset Owner advised of named responsible officer for HCS [name redacted]	REDUCED	

### 5.7 Data Protection Rights

Data protection legislation gives data subjects various rights (listed below). Limiting or restricting any of these rights is likely to be a significant impact so the justification for any restriction, as well as mitigations, must be fully outlined.

Consider each of the rights listed below and assess whether data subjects would be able to fully exercise these rights. For example:  
If an individual makes a subject access request, will you be able to easily identify, retrieve and extract the data to provide to your Data Champion?

Describe the source of risk and the nature of potential impact on individual's data protection rights.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Right to be informed not adequately covered	Remote	Minimal impact		See section 5.1	REDUCED	

[Type here]

Right of access not adequately covered and SARs cannot be properly managed and information cannot be disclosed fully	Remote	Some impact		SARs will continue to be managed by HCS Information Governance who will require access to the interface in the event of a request	REDUCED	
Right to rectification	Reasonable / Probable	Serious Harm		Supplier assured process for this – particularly as mistakes in recording can lead to a health professional not being able to appropriately assess clinical risk	REDUCED	
Right to erasure cannot be offered	Not applicable in this instance					
Right to restrict processing is not offered and data is shared with third parties against the wishes of the individual	Reasonable / Probable	Some impact		Supplier assured process in place. All secondary use to be consented UNLESS there are vital interests in play or we have a statutory obligation to share.	REDUCED	

[Type here]

Rights to automated decision making and profiling	Reasonable / Probable	Some impact		Whilst the data will be used to make decisions about the care of individuals, it will not be to their detriment – readings and data input by the patient will be used to inform priority of clinic appointments, and will enable effective resourcing. Clinicians will be able, through the clinical interface, to monitor their patients daily, and as and when required. No algorithms are in use.	REDUCED	
Right to object	Patients can object to the processing and stop using the app at any time					
<b>5.8 External Data Sharing, including the involvement of other Controllers and Processors</b>						
Your processing may involve the sharing of personal data with 3 <sup>rd</sup> party individuals, organisations or agencies.						
Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Risks identified regarding the sharing of data with third parties are outlined in sections 5.1 onwards.						
<b>5.9 International Transfers</b>						
A third country is a non EU Member State, and in these circumstances there are limits to when you can share personal data.						

[Type here]

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
--------------------------------------------------------------------------------	--------------------	------------------	--------------	----------------------	--------	---------------

Not applicable in this instance

**5.10 Human Rights**

The European Convention on Human Rights sets out numerous rights and freedoms. Limiting or restricting any of these rights is likely to be a significant impact and result in a residual high risk so the justification for any restriction, as well as mitigations, must be fully outlined. If your actions will interfere with any of the rights listed below then you must clearly outline why it is necessary and proportionate.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
--------------------------------------------------------------------------------	--------------------	------------------	--------------	----------------------	--------	---------------

The self-management of long-term conditions, the ability to be constantly monitored by clinicians and remote-care provision during the Covid-19 pandemic supports human rights, allowing people to be cared for, and kept safe.

When the pandemic is declared over, the app will still be used. Its continued use will supplement care for long term conditions.

There may be patients that would wish to use the app but who have physical needs that prevent them from being able to use the technology required. Options for patients should be explored to ensure that we are making health tools accessible to all islanders. HCS should also consider the impact on those that cannot afford or who otherwise do not have access to the tools required to use the App.

**5.11 Additional Risk Factors**

Describe any further risks, ensuring that any risks not already identified are included.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
--------------------------------------------------------------------------------	--------------------	------------------	--------------	----------------------	--------	---------------

[Type here]

**Section 7 – Outcome, Actions Prior to Implementation and Review**

Information Governance Lead [name redacted] 08/05/2020	There has been a significant amount of work undertaken to address the concerns raised regarding use of this app. These concerns have centred around the supplier’s lack of information security accreditation. MyMHealth have since undertaken the Cyber Essentials + certification, and were therefore approved by the Design Authority. Consent is the legal basis for the processing of the data, and this will continue to govern the data throughout its lifecycle. Any use for secondary purposes (unless we have a statutory obligation to do so) will be based on consent. Future plans for integration and any use of the data for research should be referred back to Information Governance and the Ethics Committee respectively.
Caldicott Guardian John McNerney 08/05/2020	
Residual risks approved by (Information Asset Owner): [Name redacted] 08/05/2020	
Project Manager [name redacted] 08/05/2020	

**Review**

A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.

[name redacted] – IG

Review 1 – Post-implementation of Phase 1

Review 2 – Pre-implementation of Phase 2

[Type here]

Section 8 – Record Keeping

The final DPIA should remain with Information Governance.  
A copy should be forwarded to the CDPU where a central register will be maintained.

Date copy forwarded to CDPU at [dataprotection2018@gov.je](mailto:dataprotection2018@gov.je) and by whom:

Date received in CDPU and by whom:

DD/MM/YYYY

[Type here]