Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your plan to use data and to help manage any potential harm to individuals' in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

There are a number of situations where a DPIA **must** be completed or where a DPIA is a **legal requirement**. If you can tick against any of the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, you must ensure that you document the reasons for your decision and discuss them with the CCG IG Lead. Regarding existing projects or programmes - a new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

ALL PROJECTS need to complete the following screening questions:

	Tick or leave blank
Use **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	☐
Process **special-category data or criminal-offence data on a large scale**;	☐
Monitor a publicly accessible place on a large scale;	☐
Use **innovative technology** in combination with any of the criteria in the European guidelines;	✓
Carry out **profiling** on a large scale;	☐
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	☐
Combine, compare or match data from multiple sources;	☐
Process personal data **without providing a privacy notice** directly to the individual in combination with any of the criteria in the European guidelines;	☐
Process personal data in a way that involves **tracking** individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	☐
Process **children's** personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	☐
Process personal data that could result in a **risk of physical harm** in the event of a security breach.	✓

Plan any major project involving the use of personal data;	☐
Plan to do evaluation or scoring;	☐
Want to use systematic monitoring;	☐
Process sensitive data or data of a highly personal nature;	☐
Processing data on a large scale;	☐
Include data concerning vulnerable data subjects;	☐
Plan to use innovative technological or organisational solutions;	✓

The Data Protection Officer[1] can be consulted before completing a DPIA in for advice and guidance or simply to talk things through. On completion, send the template to the CCG's IG Lead[2] for comment and approval by the DPO and Senior Information Risk Officer.

You MUST ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant. This DPIA can be disclosed if requested under the Freedom of Information Act (2000).

[1] Lynn Casey-Sturt lynn.casey-sturt@nhs.net

[2] Stuart Ireland stuart.ireland@nhs.net

Background Information	
Date of your DPIA :	01/07/2023
Title of the activity/processing:	Health Portal, Health Pod, Surgery Pod
Who is the person leading this work?	[redacted]
Who is the Lead Organisation?	BOB ICB
Who has prepared this DPIA?	[redacted] / EVANS Trouno (Project Lead)
Who is your Data Protection Officer (DPO)?	[redacted] [redacted] DPO for GP Practices BOB
Describe what you are proposing to do: (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	HealthPod provides a way in which Clinicians can obtain relevant measurements relating to their patients. With minimal clinical involvement, the measurements can then be automatically collected and filed in the patients' GP medical record for clinical review. Alerts (when configured) are then generated where readings are abnormal. Self-Check-In provides a way for patients to check-in to attend appointments without interacting with practice staff members, using an All-In-One Touchscreen. The system automatically updates the Clinical Management System that the patient has arrived for their appointment. The benefit of the products in the HealthPortal solution is that it relieves reception staff of checking patients in for their appointments and healthcare professionals of obtaining relevant measurements relating to their patients and therefore allows practice staff to focus on other important patient facing services/care.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is)**.**	Microtech Group Limited/ GP Practice(s)/Surgeries and BOB ICB.
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	None.
Detail anything similar that has been undertaken before?	Health Portal/Health Pod/Surgery Pod is a Commercially Off The Shelf (COTS) telehealth system and has been rolled out to many GP Practices and Surgeries across the UK.

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use

1.1.

What data/information will be used? Tick all that apply.	Tick or leave blank	**Complete**
Personal Data	✓	1.2
Special Categories of Personal Data	✓	1.2 AND 1.3
Personal Confidential Data	✓	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data)	☐	1.2 but speak to your IG advisor first

Pseudonymised Data	☐	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	☐	Consider at what point the data is to be anonymised
Commercially Confidential Information	☐	Consider if a DPIA is appropriate
Other	☐	Consider if a DPIA is appropriate

1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:

a) THE DATA SUBJECT HAS GIVEN CONSENT — **Tick or leave blank** ☐

Why are you relying on consent from the data subject?

What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom).

Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this).

Comply as per our Data Protection policies and procedures.

b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY — **Tick or leave blank** ☐

(The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).

What contract is being referred to?

c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT — **Tick or leave blank** ☐

(A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).

Identify the legislation or legal obligation you believe requires you to undertake this processing.

d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON — **Tick or leave blank** ☐

(This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).

How will you protect the vital interests of the data subject or another natural person by undertaking this activity?

Click here to enter text.

e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	**Tick or leave blank** ✓
What statutory power or duty does the Controller derive their official authority from? **Health Care Act 2012 Sec 3a (1) Each integrated care board may arrange for the provision of services or facilities as it considers appropriate for the purposes of the health service that relate to securing improvement.**	
f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	**Tick or leave blank** ☐
What are the legitimate interests you have? Contract: the processing is necessary for Microtech to deliver on the obligations on the contract.	

Article 9 (2) conditions are as follows:

a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	**Tick or leave blank** ☐
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available). N/A	**Tick or leave blank** ☐
c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	**Tick or leave blank** ☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*
e) The data has been made public by the data subject	*NA*
f) For legal claims or courts operating in their judicial category	*NA*
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE OR OCCUPATIONAL MEDICINE, FOR THE ASSESSMENT OF THE WORKING CAPACITY OF THE EMPLOYEE, MEDICAL DIAGNOSIS, THE PROVISION OF HEALTH OR SOCIAL CARE OR TREATMENT OR THE MANAGEMENT OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ✓
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT. (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

1.3.

If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to j). NOTE: d), e) and f) are not applicable

1.4.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
Microtech Group Limited	Processor
BOB (25 Selected GP Practices & Surgeries)	Sole Controller
BOB ICB	Other
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

1.5.

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

The HealthPortal; HealthPod solution is accessed directly by patients and collects data from them through a mix of data input (e.g. – Asthma Review/Smoking/Alcohol consumption) and automated data readings (e.g. - Blood Pressure) after which the data collected will be automatically populated into the patient's GP medical record. The data will give the clinicians informed health readings for the patient before an appointment for a face-to-face meeting is set. The health readings that are collected can trigger an alert if it exceeds a pre-set threshold for the clinicians to take any urgent action(s) to meet with the patient.

The HealthPortal; Self-Check-In solution is accessed directly by patients and allows them to Self-Check-In for their GP appointment using a patient Self-Check-In, All-In-One Touchscreen or personal mobile device. The HealthPortal/Check-In system automatically updates the Clinical Management System that the patient has arrived for their GP appointment.

The data is stored within the secure Microsoft Azure cloud platform.

The data will not be shared with any third parties unless Microtech are instructed to do so on behalf of the Data Controller and the DPIA is updated.

Microtech staff will only have access to patient identifiable data when this is necessary to resolve system issues, and this is typically a rare event.

1.6.

Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)

Information acquired by the Health portal/Health Pod/Surgery Pod on the patient including patient vital signs and health protocol questionnaire information.

1.7.

How are you satisfying the common law duty of confidentiality?

Consent – Implied if a confidential patient information is captured using the surgery pod, accessed and used for their individual care then their consent is implied, without them having to explicitly say so.

If you have selected an option which asks for further information please enter it here

Although Consent is implied through the act of using the health portal/Health Pod/Surgery Pod. An explicit consent message can be enabled in line with BOB ICB/Individual Practice consent rules.

1.8.

Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?

Yes

If you are then describe what you are doing.

For analysis purposes for the ICB anonymisation can be applied. Data is encrypted.

If you don't know then please find this information out as there are potential privacy implications with the processing.

1.9.

Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ✓

If so describe that purpose.

For analysis purposes with ICB related work

1.10.

Approximately how many people will be the subject of the processing?

1000 plus

1.11.

How are you collecting the data? (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)

Electronic form

Choose an item.
Choose an item.
Choose an item.

If you have selected 'other method not listed' describe what that method is.

Click here to enter text.

1.12.

How will you edit the data?

Microtech will not be editing the data as that will affect the data integrity. The data will not be editable on the surgery pod as captured data will be directly posted to the patient clinical records.

1.13.

How will you quality check the data?

Reviewed by Health professionals and clinicians.

1.14.

Review your business continuity or contingency plans to include this activity. Have you identified any risks?

No

If yes include in the risk section of this template.

1.15.

What training is planned to support this activity?

Full training is provided to mitigate any risks.

2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

2.1.

Are you proposing to combine any data sets?

No

If yes then provide the details here.

Click here to enter text.

2.2.

What are the Data Flows? (Detail and/or attach a diagram if you have one).

Microtech - HealthPortal Technical Architecture Workflow.pdf

2.3.

What data/information are you planning to share?

The data will not be shared with any third parties unless Microtech are instructed to do so on behalf of the Data Controller and the DPIA is updated.

Microtech staff will only have access to patient identifiable data when this is necessary to resolve system issues, and this is typically a rare event.

2.4.

Is any of the data subject to the National Data Opt Out?

No - it is not subject to the national data opt out

If your organisation has to apply it describe the agreed approach to this

Click here to enter text.

If another organisation has applied it add their details and identify what data it has been applied to

Click here to enter text.

If you do not know if it applies to any of the data involved then you need to speak to your Data Protection Officer to ensure this is assessed.

2.5.

Who are you planning to share the data/information with?

The data will not be shared with any third parties unless Microtech are instructed to do so on behalf of the Data Controller and therefore, the DPIA will then be correctly updated. Microtech staff will only have access to patient identifiable data when this is necessary to resolve system issues. This type of event is rare and typically never occurs.

2.6.

Why is this data/information being shared?

The data will not be shared with any third parties unless Microtech are instructed to do so on behalf of the Data Controller and therefore, the DPIA will then be correctly updated. Microtech staff will only have access to patient identifiable data when this is necessary to resolve system issues. This type of event is rare and typically never occurs.

2.7.

How will you share it? (Consider and detail all means of sharing)

The data will not be shared with any third parties unless Microtech are instructed to do so on behalf

of the Data Controller and therefore, the DPIA will then be correctly updated. Microtech staff will only have access to patient identifiable data when this is necessary to resolve system issues. This type of event is rare and typically never occurs.

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements ☐

Provide details of how you have considered any privacy risks of using one of these solutions

Hazard Log 1.2.3.xlsx

.

2.8.
What data sharing agreements are or will be in place?
Data sharing agreement will be based on the ICB agreement with the practices and the selected GP practices

2.9.
What reports will be generated from this data/information?
Analytic information, including usage, protocol information, demographic information, etc. can be reported via the Health Portal Dashboard for the practice use and analysis. Information focused on usage and QOF achievement maybe requested by the ICB periodically to make informed decision and for audit purpose ensuring there is no breach in data confidentiality.

2.10.
Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?
No

If yes, are all the right agreements in place?

Give details of the agreement that you believe covers the use of the NHSD data
NHS IM1.

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1
Are you proposing to use a third party, a data processor or a commercial system supplier?
Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.
Microtech Group Limited
17-19 Hill Street
Kilmarnock
KA3 1HA
Click here to enter text.
Click here to enter text.
Click here to enter text.
Click here to enter text.
Click here to enter text.

3.2
Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
Microtech Group Limited	Yes	Registration Reference ZA431325
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

3.3

What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
Microtech Group Ltd	Certification No. 72389, ISO9001 Certified, ISO27001, Certificate No. 185782, Cyber Essentials Certified - Certification No. IASME-CE-008048
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

3.4

What is the status of each organisation's Data Security Protection Toolkit?

DSP Toolkit

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Microtech Group Limited	8JF05	Standard Met	24th Aug 2022
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

3.5

How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

The data is stored within the secure Microsoft Azure cloud platform.

Microtech - HealthPortal Technical Architecture Workflow.pdf

3.6

How is the data/information accessed and how will this be controlled?

Microtech - HealthPortal Technical Architecture Workflow.pdf

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.
The Microsoft Azure platform is used to deliver Health Portal and has a strong reputation as a flexible, reliable, and secure service. There are currently no known security issues or issues of public concern to be factored in.

3.8
What security measures will be in place to protect the data/information?
The Data Processor (Microtech) operates according to GDPR and Data Protection standards. The Data Processor is registered and compliant with the NHS Digital Data Security and Protection Toolkit and is compliant with the following standards: Cloud Computing Standards (via Microsoft Azure), Cyber Essentials (CE) certification and ISO27001 Information Security Management accreditation.
Microtech also hold the following accreditations: -
ISO9001 Certified. Certification No. 72389.
ISO27001 – Certificate No. 185782.
Registered with ICO for data protection. Registration No. ZA431325.
Data Security & Protection Toolkit, formally IG Toolkit compliant. Org Code 8Jf05
Cyber Essentials Certified.
Certification No. IASME-CE-008048.

Is a specific System Level Security Policy needed?
No

If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

3.9
Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information).
No

If yes describe where and what additional measures are or will be in place to protect the data.

3.10
What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?

MICROTECH GROUP LTD DATA PI

4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

4.1
Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date? (There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).
Changes to privacy notice will be updated and distributed by the selected GP practices.

4.2
How will this activity impact on individual rights under the GDPR? (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).
This activity will not impact on the individual rights as patients as the responsibility stays with the data controller.

4.3
How long is the data/information to be retained?
For the length of the contract with Microtech data will be retained under the data controller policies.

4.4
How will the data/information be archived?

For the length of the contract with Microtech data will be retained under the data controller policies.

4.5

What is the process for the destruction of records?

When customers terminate a contract, we follow strict standards for deleting data. In collaboration with Microsoft Azure, Microtech executes a complete deletion of data on termination of contract or on customer request.

4.6

What will happen to the data/information if any part of your activity ends?

Microtech will consult with BOB ICB and the selected GP practices if this occurs.

4.7

Will you use any data for direct marketing purposes? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes please detail.

Click here to enter text.

5. Risks and Issues

5.1

What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks.

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Patient may enter invalid information	Possible	Minimal	Medium
Device takes patient readings which may be broken	Possible	Minimal	Medium
Protocol results sent to data centre, the information sent may become corrupted	Possible	Minimal	Low
Patient visits surgery for another reason and then uses SurgeryPod and checks Blood Pressure, which is abnormally high.	Possible	Minimal	Low
Details validated against patient store in cloud, validation rules fail to apply correctly	Possible	Minimal	Low

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Patient is able to enter invalid values	Most protocols do not rely on the patient entering complex data directly. Either data is collected from a medical device or patient is presented with a selection of options from which they	Eliminated	Low	

	must choose. In the rare circumstances where a patient may be required to enter complex data, the values are validated to ensure they fall within a suitable range for the data item in question. Proposed System Change: Where complex data is manually entered rather than collated from a medical device, the protocol notes it was a manual entry and this can be sent by medical professionals when they review the results.			
Device takes patient readings which may be broken	Data collected from medical devices is validated to ensure it falls within an acceptable range for the data item. Medical devices are calibrated prior to delivery to customer. It is made clear to Organisations that they are responsible for the calibration and servicing of any medical devices provided by Microtech.	Reduced	Low	
Protocol results sent to data centre, the information sent may become corrupted	HTTP traffic has corruption detection built in. Where large data is sent in the system a MD5 checksum is generated at the sending point and re-calculated at the receiving point if the two checksums do not match an error is generated and the process must be repeated.	Eliminated	Low	
Patient visits surgery for another reason and then uses SurgeryPod and checks Blood Pressure, which is abnormally high.	When we deliver a system, we get the practice/clinical staff to advise of specific thresholds/parameters that are set within the systems, eg. BP thresholds. Alerts are then triggered and notify admin/clinical staff of any breach of threshold/parameters. For	Eliminated	Low	

	example this can happen in the case of a dangerously high value BP reading which may be detected in a patient. In such a case, (and as previously mentioned) an alert is immediately triggered and notifies practice staff of the threshold breach and/or the patient is advised to go to reception straight away.			
Details validated against patient store in cloud, validation rules fail to apply correctly	Unlikely as error capturing in place for rules validation and UAT will establish that this works before go Live	Eliminated	Low	Choose an item.

5.3
What if anything would affect this piece of work?
N/A

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
Click here to enter text.

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
No

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (You may need the help of your DPO with this)
No

If yes, explain why you have come to this conclusion.
Click here to enter text.

7. Data Protection Officer Comments and Observations

7.1 **Comments/observations/specific issues**	DPO GP Comment : 08.02.2024 – Further to the review of this DPIA and discussion with IG Consultant – GP Practices Privacy Policy to be updated to reflect this processing of data by MicroTech. Furthermore to be confirmed with the Head of Digital Delivery if DTAC needs to be completed as it involves technology solution. BOB ICB DPO: On the basis the above advice is undertaken, no further actions required

8. Review and Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:
A) There are no further actions needed and we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection
Click here to enter text.

We believe there are
Choose an item.

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board

Name: [redacted]

Job Title: Governance Manager and Data Protection Officer

Signature: [redacted] Date: 14/02/2024

Signed and approved on behalf of Click here to enter text.

Name: Click here to enter text.

Job Title:

Signature: Click here to enter text. Date: Click here to enter a date.

Please note:

You MUST ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here: Click here to enter text.