Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your processing 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.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:	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.	☐

You as Controller should **consider** carrying out a DPIA where you	Tick or leave blank
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;	✓

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.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
Date of your DPIA :	22/07/2022
Title of the activity/processing:	Deployment of Minuteful Kidney as a Service using the ACR App with Healthy.io as Processor
Who is the person leading this work?	[redacted], Clinical Lead
Who is the Lead Organisation?	BOB ICB – BW Place
Who has prepared this DPIA?	[redacted], Long Term Conditions Transformation Lead, former BWCCG [redacted], Long Term Conditions Transformation Manager, former BWCCG
Who is your Data Protection Officer (DPO)?	[redacted], DPO, BOB ICB [redacted], IG Consultant, Corporate Services, NHS South, Central and West
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).	Healthy.io has created Minuteful Kidney as a Service to support general practice and other NHS providers monitor patients at risk of chronic kidney disease. In this process, primary care practices will supply Healthy.io with a list of patients that have not engaged with the annual kidney function screening offered by the practice as part of the patient's care pathway. Patients will be invited to use an App in order to check a sample of their Urine using a specific test kit that will be sent to them. The results will be sent to the registered GP for review and addition to the Patient record.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	Healthy.io (Data Processor) GP Practices (Data Controller) Sub-processors (Data Processors)
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	Relevant former CCGs where they were the commissioners of the service on behalf of their Practices. Berkshire West GP IT Committee will be involved for oversight from an IT/digital purpose.
Detail anything similar that has been undertaken before?	The Service/approach has either been and/is being offered in former Bucks CCG and former Oxfordshire CCG. It has reportedly been delivered in other former CCGs across the TV areas.

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?
Consent needs to be obtained from the patient in providing some data to Healthy-io in order for the patient to receive the test kit.

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

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

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?
Click here to enter text.

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.
Click here to enter text.

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 — Tick or leave blank: ✓

(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).

What statutory power or duty does the Controller derive their official authority from?
Article 6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (for processing under a public body contract);

The Practice is contracted to manage the care for Patients with diabetes in accordance with the NHS RightCare » Diabetes pathway (england.nhs.uk) and does so under the NHS Act 2006 as amended by the Health and Social Care Act 2012 and other relevant acts and directions for providing primary care services.	
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? Click here to enter text.	

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).	**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	**Tick or leave blank** ☐

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).	

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
GP Practices	Sole Controller
Healthy.io	Processor
Sub-processors contracted via Healthy-io (See table on Page 9)	Sub-Processor
	Processor
	Processor
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?

There are nine recommended care processes identified as important markers of improved long-term care of patients with diabetes. Of the nine, two involve offering annual Kidney function testing (Urinary albumin and Serum creatinine) NHS RightCare » Diabetes pathway (england.nhs.uk). Primary Care Practices will be able to offer a test that a Patient can carry out in the comfort of their own home with the hope of increasing engagement with Patients who find it hard to attend for this annual test and/or choose to use this approach.

The GP practice will identify the eligible patient cohort by importing the EMIS/SystmOne search template provided by Healthy.io (see EMIS ACR Search Template). The search template automatically generates a list of patients, automatically removing those who are not eligible for the service. The default inclusion criteria are patients with diabetes who have missed their annual ACR test. The exclusion criteria are patients who are pregnant; live in a care home; have a catheter in-situ; are at the end of their life or on renal replacement therapy.

The practice sends these eligible patients an SMS using MJOG/AccuRx or other messaging platform informing them that their details will be shared with Healthy.io (see SMS Patient template for wording). Participants are given 1 week after the introductory text to decline the service. The GP practice will then remove from the automatically generated list, the patients who have opted out. Practices will also be advised to make sure any patients that have a Type 1 opt out (93C1) or GDPR opt out (9NU0) coded on their record are not included on the list to be provided to Healthy.io. The remainder of the list is now automatically generated into a report that can be sent to Healthy.io via the approved Healthy.io NHS email account. This list is reviewed by Healthy.io and uploaded to the Healthy.io portal and Healthy.io's team will begin contacting patients over the phone to offer a home-based test.

Within this phone call, Healthy.io will obtain the patient's willingness to participate, confirm their address and mobile number, and send a link to download the app to their mobile phone number via SMS; further information about this is available at ACR Digital Urinalysis app - NHS (www.nhs.uk). The address will then be passed on to Healthy.io's distribution partner, Precision, who will post the kit to the patient's home address. Once the patient has downloaded the app and received the Healthy.io ACR test kit, they will run the ACR test independently. At the end of the analysis the test results are automatically added to the patient record in the Healthy.io portal. This result is then shared with the GP via MESH into the patient's electronic medical record.

It is important to note that in this Healthy.io model, patients are not required to create an account; the app is downloaded and is linked by the mobile phone number. The results return to the device and are accessed through the app. Once a patient deletes the app, the results stored locally on their device are deleted. The results are however kept for analytical purposes by Healthy.io but in anonymised form.

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)

Clinical test results

1.7.

How are you satisfying the common law duty of confidentiality?

Consent - Implied

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

In regard to the Common Law Duty of Confidentiality, as this is a GP provided service to support individuals with their direct care, it is considered that implied consent can be relied upon. Implied consent can be relied upon where the use of confidential data is used for direct care and where the individual would have a reasonable expectation that their confidential data will be used in that way. To support this, once eligible patients are identified by the GP Practice, they shall be sent an SMS which informs them the GP Practice has asked Healthy.io to support them in delivering the service, and be given the opportunity to decline. Healthy.io will then only contact that patient on behalf of the GP if they have not declined to be part of this service or have not responded.

For example, the SMS message could read:
As part of your annual diabetes care, we have asked Healthy.io, who are part of a national NHS programme, to contact you to discuss sending you a home urine test to check your kidney function. For more about the test please visit: https://bit.ly/NHS-ACR. More information about why we are doing this can be found at GP link to privacy notice. If you do not want us to share your details with Healthy.io, reply back "No" and your full name to this message by the ……date tbc…….. Thank you, XXX Medical Centre.

When Healthy.io contact the Patient, they will be given another opportunity to decline the service and then Healthy.io will maintain a suppression list for the duration of the contract of those who do not wish to be part of the programme to ensure that once they are opted out, they are not contacted again, consistent with ICO advice on suppression list and the right to object. This will be destroyed at the end of the contract.

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.

Healthy.io will anonymise information for analytics purposes.

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.

Healthy-io states the following:
The Controller acknowledges and agrees that Healthy.io shall be able to use and disclose Anonymised Data in its sole discretion for Healthy.io's own legitimate business purposes (e.g.: testing, developing, improving and operating the services / products) without restriction. Personal Data will be rendered fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognised by Data Protection Legislation in such a manner that the Data Subject is not or no longer identifiable. Data Protection Legislation does not apply to Anonymised Data

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.)

By text
By telephone
Electronic form

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?

Data will be edited to remove Patients who decline the service being offered by Healthy.io, this will be done before the contact details are shared with Healthy.io by the practice. Where a patient declines when contacted by Healthy-io, processes are in place

1.13.

How will you quality check the data?

The Practice will subject the data to their own procedural quality checks prior to sharing data with Healthy-io e.g. active patient registration.

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?

Instructions will be provided to the Practice on how to set up the arrangements with Healthy-io. Healthy-io have offered to provide support with onboarding e.g. GP webinar, as well as face to face training at individual practices.

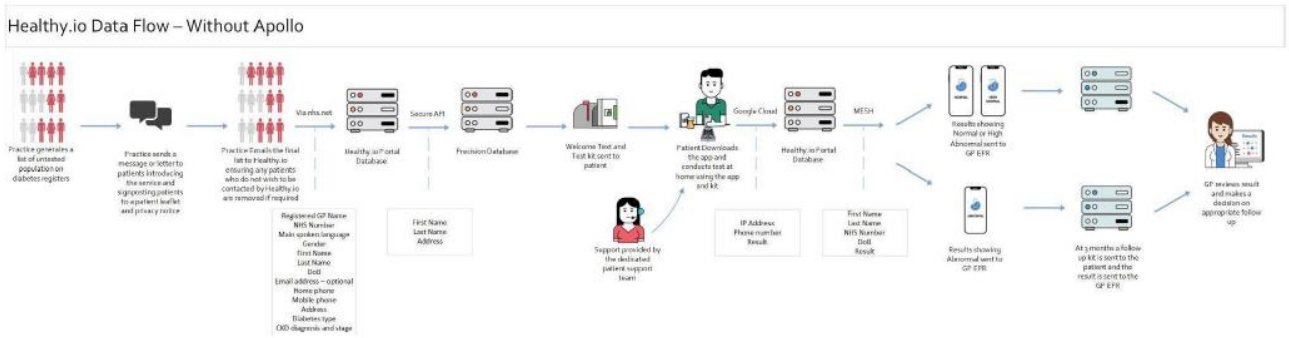
2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

2.1.

Are you proposing to combine any data sets?
Yes

If yes then provide the details here.
Healthy-io will undertake an evaluation of the outcomes and perceived benefits. This will include anonymised data, categorised by age, gender, ACR outcomes etc.

2.2.
What are the Data Flows? (Detail and/or attach a diagram if you have one).



2.3.
What data/information are you planning to share?

1. Precision will process the data subject name, address, and telephone details only for test kit delivery purposes only. Name, address and telephone number are shared with our distribution partner Precision **https://www.precision.co.uk/** Precision uses West Europe, North Europe, and UK data centres.
2.
3. Person identifiable data is stored in a separate database to test data.

The data processed is:
- Registered GP Name
- NHS Number
- Main spoken language
- Gender
- First Name
- Last Name
- DoB
- Email address – optional
- Home phone
- Mobile phone
- Address
- Diabetes type
- CKD diagnosis and stage
- Date and value of last ACR test
- Smartphone information - Carrier, OS, Device, model,

App version, City
- App information – IP Address

● Test Date
● Test Result

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?
Data will be shared between GP Practices and Healthy-io, and between Healthy-io and their sub-processors.
Anonymised evaluation data will be used to inform BOB ICB of the outcomes of the project.
Healthy-io states that their employees, in authorised roles, will have access to the data:

● Partnership & Programmes Lead or Manager - to support practices with deployments e.g., generating the patient list.

● Patient Onboarding Operator - to support patients with downloading and using the application and test kit.

● Product Owner - to liaise with customers to understand a bug or workflow issue and to support the technical team with troubleshooting bugs and issues.

● Technical Developer - to troubleshoot bugs and issue.

2.6.
Why is this data/information being shared?
For evaluation purposes and for patient care.

2.7.
How will you share it? (Consider and detail all means of sharing)
By text, telephone, Electronic form and written evaluation.

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
Click here to enter text.

2.8.
What data sharing agreements are or will be in place?
Each individual practice will agree and sign a Data Protection Agreement with Healthy-io, if they wish to take part.

2.9.
What reports will be generated from this data/information?
Anonymised data will be used to report and evaluate the outcomes of the project for former BWCCG. Patient ACR-reported outcomes will be shared directly with their practice.

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?
Choose an item.

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

Click here to enter text.

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.

Sub-Processors, International Transfers

Minuteful Kidney Healthy.io Approved Sub Processors and International Transfers					
Name	**Relationship to Healthy.io**	**Purpose of Processing**	**Type of data**	**Location of processing**	**Safeguards**
Google	Data processor	Hosting, Storage, Database, Networking	Personal identifiable data and special category data	UK and EU	DPA & Privacy Policy
Google	Data processor	Identity management	Mobile phone numbers for identification	US	Standard Contractual Clauses (SCC), DPA & Privacy Policy
Precision Marketing Group	Data processor	Fulfilment services	Name, address, and telephone number only	EU	DPA & Privacy Policy
Twilio	Data processor	SMS centre	Name and mobile phone number	US	Standard Contractual Clauses (SCC), DPA & Privacy Policy
Amazon Web Services	Data processor	HSCN Hosting	Personal identifiable data and special category data	EU	DPA & Privacy Policy
Coralogix	Data processor	Logging and monitoring	IP Address	US	Standard Contractual Clauses (SCC), DPA & Privacy Policy
3cx (SheshTech)	Data processor	Telephony Software	Personal identifiable data only	EU	DPA & Privacy Policy
Freshworks	Data processor	Customer Support CRM	Mobile phone number, freestyle text the user can submit	EU	DPA & Privacy Policy
Melissa	Data processor	Address validation	Home address	EU	DPA & Privacy Policy

Please note

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
Healthy.io	Yes	**Registration number:** ZA289700 **Date registered:** 26 October 2017 **Registration expires:** 25 October 2021 **Payment tier:** Tier 1 **Data controller:** Healthy.io (UK) LTD **Address:** Kings Fund 11-13 Cavendish Square London W1G 0AN
Precision	Yes	ZA729836
Google UK	Yes	Z6647359
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
Healthy.io	DPIA, DPA and DTAC (DTAC not reviewed due to lack of formal governance route) provided by Healthy-io, including contractual relationship with all sub-processors. A contract has been signed between Healthy-io and former Berkshire West CCG. However, this is not a standard NHS contract.
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.

3.4

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
Healthy.io	8KC08	Standards met	20/05/2020
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).

Healthy-io state in their DPIA that data is stored on Google Cloud UK servers. They state that Google Cloud services hold a vast array of security and privacy certifications, see link to Google's compliance and data processing pages below.

https://cloud.google.com/security/compliance

https://cloud.google.com/terms/data-processing-terms

Healthy.io have stated they have a team based in Israel who will have access to personal data to manage the Minuteful Kidney product and states that Israel is a country covered by the UK Adequacy Regulations.

Healthy-io states that no data is stored to patient's mobile devices.

3.6

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

Healthy-io states that data access controls are:

- Staff training and awareness
- Employment contract responsibilities specifies compliance with company policies and regulations.
- Unique username and passwords
- Access only granted to authorised roles (see point 11)
- Security monitoring policy

Healthy-io states the following measures are in place to protect the data:

- ICO registered - ZA289700.
- Access controls based on the 'Principle of least privilege'.
- Strong and complex password requirements and controls to enforce are in place.
- Security monitoring policy
- Only appointing sub-processors who can provide sufficient security guarantees.
- ISO 27001 certification achieved - IL - 86650.
- Data Protection & Security Toolkit standards met – 8KC08.
- Sensitive data is AES 256 encrypted at rest
- Data in transit is encrypted TLS v1.2

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

Healthy-io state in their DPIA that data is stored on Google Cloud UK servers. They state that Google Cloud services hold a vast array of security and privacy certifications, see link to Google's compliance and data processing pages below.

https://cloud.google.com/security/compliance

https://cloud.google.com/terms/data-processing-terms

3.8

What security measures will be in place to protect the data/information?

Healthy-io states the following measures are in place to protect the data:

- ICO registered - ZA289700.
- Access controls based on the 'Principle of least privilege'.
- Strong and complex password requirements and controls to enforce are in place.
- Security monitoring policy
- Only appointing sub-processors who can provide sufficient security guarantees.
- ISO 27001 certification achieved - IL - 86650.
- Data Protection & Security Toolkit standards met – 8KC08.
- Sensitive data is AES 256 encrypted at rest
- Data in transit is encrypted TLS v1.2

Is a specific System Level Security Policy needed?

Don't know

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)

Yes

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

Minuteful Kidney Healthy.io Approved Sub Processors and International Transfers					
Name	**Relationship to Healthy.io**	**Purpose of Processing**	**Type of data**	**Location of processing**	**Safeguards**
Google	Data processor	Hosting, Storage, Database, Networking	Personal identifiable data and special category data	UK and EU	DPA & Privacy Policy
Google	Data processor	Identity management	Mobile phone numbers for identification	US	Standard Contractual Clauses (SCC), DPA & Privacy Policy
Precision Marketing Group	Data processor	Fulfilment services	Name, address, and telephone number only	EU	DPA & Privacy Policy
Twilio	Data processor	SMS centre	Name and mobile phone number	US	Standard Contractual Clauses (SCC), DPA & Privacy Policy
Amazon Web Services	Data processor	HSCN Hosting	Personal identifiable data and special category data	EU	DPA & Privacy Policy
Coralogix	Data processor	Logging and monitoring	IP Address	US	Standard Contractual Clauses (SCC), DPA & Privacy Policy
3cx (SheshTech)	Data processor	Telephony Software	Personal identifiable data only	EU	DPA & Privacy Policy
Freshworks	Data processor	Customer Support CRM	Mobile phone number, freestyle text the user can submit	EU	DPA & Privacy Policy
Melissa	Data processor	Address validation	Home address	EU	DPA & Privacy Policy

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?

A data processing agreement between the Practice (as data controller) and Healthy.io will be in place, if the practice choose to take part.

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).

Healthy-io state that patients are informed about the purpose of collection and use of their personal data via the initial text or letter from their practice which includes a link to the practice privacy notice. The Data Controller is responsible for informing their patients about new data processing in advance of the new data processing taking place and signposting the patient to their privacy notice.

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)

Healthy-IO states that individual rights requests are the responsibility of the data controller. Any individual rights requests that are made directly to Healthy-io will be reported to the data controller for the data controller to process and confirm actions required to be taken by Healthy-io.

4.3

How long is the data/information to be retained?

Healthy-Io states that data will be retained only until the Patient agrees to participate in the Healthy.io which is confirmed during the telephone call with Healthy.io. Should the Patient decline, their data will be deleted by Healthy.io. Once participating in the service, Patient information will be retained by Healthy.io for the duration of the contract wherein it will be securely removed from Healthy.io servers and where necessary, returned to the Controller. Results are kept by Healthy-io for analytic purposes in an anonymised form. When the app is uninstalled from the user's device, the local information is deleted. However, a copy of the results stays available to Healthy-io and can still be linked back to the individual. The IP address is kept by Healthy-io stated purely for system maintenance and security purposes. It is stated by the organisation that this will be used for no other purpose and destroyed after 1 year. All data is subject to Healthy.io's data retention policy QSR 2811/01. Healthy.io will retain the patient data they receive for the shorter of: (i) Minimum time required under applicable law or (ii) duration of contract, and in any event no longer than 7 years.

4.4

How will the data/information be archived?

Healthy-io product team to confirm archiving arrangements. The data will not be archived except where this is required. Healthy-io state they work in line with NHS IG rules and regulations including the Records Management Code of Practice; for the Minuteful Kidney service, we will be acting under a Data Processing Agreement (DPA) with Practices; the DPA outlines our Data Protection obligations.

4.5

What is the process for the destruction of records?

Healthy-io state All data is subject to Healthy.io's data retention policy QSR 2811/01. Healthy.io will retain the patient data they receive for the shorter of: (i) Minimum time required under applicable law or (ii) duration of contract, and in any event no longer than 7 years.

All data is subject to Healthy.io's data disposal policy QSR 2811/00. In this instance as the data is solely stored electronically at termination of the contract an anonymised data extract will be retained by Healthy.io and all other person identifiable data will be erased from all Healthy.io databases.

4.6

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

The data will be deleted by Healthy.io.

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.

Likelihood		Severity	
1	Rare	1	Negligible
2	Unlikely	2	Minor
3	Possible	3	Moderate
4	Likely	4	Major
5	Almost certain	5	Catastrophic

LIKELIHOOD	IMPACT / CONSEQUENCES				
	NEGLIGIBLE 1	LOW 2	MODERATE 3	SIGNIFICANT 4	EXTREME 5
1 (rare)	L	L	M	H	H
2 (unlikely)	L	L	M	H	E
3 (possible)	L	M	H	E	E
4 (likely)	M	M	H	E	E
5 (almost certain)	M	H	E	E	E

Risk Description	Impact	Likelihood	Risk Score	Proposed Risk solution (Mitigation)
Inaccurate patient information may lead to unwarranted contact	4	1	4	Patient contact information is supplied by the data controller therefore the data controller will mitigate this risk by ensuring patient data is as accurate and up to date as possible.
Insufficient information provided to the data subject about the sharing of their data with Healthy.io	3	1	3	The data controller will mitigate this risk by sending out a text or letter introducing the service. Healthy.io will support provision of fair processing material to patients, see Appendix 3
Personal data may not be appropriately managed by sub-processors	3	1	3	The data controller mitigates this risk by completing a DPIA as part of due diligence. Healthy.io mitigate this risk by having a contract and Data sharing agreement in place with sub processors.
Identifiable information held by Healthy.io may be a risk to individual rights.	3	1	3	Healthy.io mitigates this risk by storing identifiable information for patients only for the purposed of the contracted service and for the period designated in the Records Management Code of Practice for Health and Social Care.

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**
Information is shared with Healthy IO against a patient's wishes.	Possible	Significant	Medium
Identifiable information held by Healthy IO may be a risk of information security issues	Remote	Significant	Medium
As above	Possible	Minimal	Low
As above	Possible	Significant	Medium
As above	Possible	Significant	Medium
As above	Probable	Significant	High
As above	Possible	Significant	Medium

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)**
Information is shared with Healthy IO against a patient's wishes.	The practice must remove all patients who have declined the service before sharing patient details with Healthy IO.	Reduced	Low	Yes
Identifiable information held by Healthy IO may be a risk of information security issues	Healthy IO mitigates this risk by protecting data in several ways as outlined in 3.6	Reduced	Low	Yes
		Reduced	Low	Yes

		Tolerated	Low	Yes
		Tolerated	Low	Yes
		Reduced	Low	Yes
		Reduced	Low	Yes

5.3
What if anything would affect this piece of work?
Practice choice, time and resource and Patient choice, if either wish to not participate

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
None.

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
Yes

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
Former Berkshire West CCG has worked with Healthy-io to be advised of IG arrangements between the Data Processor, Data Controller and sub-processors.

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

Practices should update their data flow map and privacy notice to make sure patients are aware of the activity.

Suggested privacy notice text:

Activity	Rationale
Home urine testing	**Purpose** - The NHS has commissioned Healthy.io, as part of a national NHS programme, to deliver a service providing at home urine test kits so patients at risk of chronic kidney disease can conduct this important test at home using a smartphone. We will contact relevant patients to tell you more about the programme and how to opt out if you don't want us to share your contact details with Healthy.io to enable them to contact you and send you a test kit. **Legal Basis**: UK GDPR Article 6(1)(e) and Article 9(2)(h) **Processor:** Healthy.io

Practices must make sure any patients that have a Type 1 opt out (93C1) or GDPR opt out (9NU0) coded on their record are excluded from the list of patients to be provided to Healthy.io.

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 DPO Support Service for BW Place GP Practices

Name: [redacted]

Job Title: IG Consultant

Signature: [redacted] Date: 21/07/2022

Signed and approved on behalf of Buckinghamshire, Oxfordshire and Berkshire West Integrated Care Board (BOB ICB)

Name: [redacted]

Job Title: Governance Manager and Data Protection Officer Signature: [redacted] Date: 22/07/2022
Please note: You should 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.