Ref- 23/24-026

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.

A) BACKGROUND INFORMATION	
Date of your DPIA :	12/02/2024
Title of the activity/processing:	Deploying an automated system ("Dora") to undertake clinical conversations with patients.
Who is the person leading this work?	[redacted], Head of Planned Care, BOB ICB
Who is the Lead Organisation?	Buckinghamshire, Oxfordshire and Berkshire West ICB
Who has prepared this DPIA?	[redacted], Transformation Support Manager, BOB ICB
Who is your Data Protection Officer (DPO)?	BOB ICB – [redacted]
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).	This project is to deploy an automated system "Dora", which is supplied by Ufonia. Dora is a UKCA-marked autonomous telemedicine platform, provided by Ufonia, that calls patients to provide and gather information. In this instance, Dora will undertake telephone calls and electronic communications to patients referred for treatment, gather information to check suitability for treatment and provide information to support patient choice to assist referral of patients on to the most clinically appropriate provider. NHS England have prioritised 'eMeet' projects to contact patients at the point of referral. To facilitate shared decision making, patients are being screened at the point of referral and offered choice of suitable providers. NHSE supports the use of digital technology to enable this in order to ensure resources are used efficiently across the system. The benefits are envisaged to: • Contact all patients at the point of referral to reassure them that their referral has been received, and give patients information about the next steps in their care pathway • Give all patients standardised and transparent choice over where they receive their treatment (based on agreed eligibility criteria) in a scalable way • Collect pre-operative assessment information to allow providers to standardise triage and save clinician time in first outpatient appointment clinics • Give patients access to early shared decision making about their care, • Promote self-service and give patients advice about the best way of managing their care via available channels
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	Yes BOB ICB, [redacted], Head of Planned Care, BOB ICB Ufonia Limited, [redacted] Buckinghamshire Health Trust, [redacted], [redacted]

	Royal Berkshire Foundation Trust, [redacted] Oxford University Hospital, [redacted] Local Optical Committee (LOC) Oxfordshire, [redacted] LOC Berkshire, [redacted] LOC Buckinghamshire, [redacted] Ophthalmology Independent Sector Providers – Newmedica, Spam edica, Circle Reading, Ramsey BIH, PEC, Ramsey Cherwell, Cherwell Hospital Rego
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	GPs/Practice Administrators, Optometrists We have engaged, informed, and consulted representatives of these groups.
Detail anything similar that has been undertaken before?	The Dora system is currently live across all NHS trusts in the BOB region at other points in the patient's pathway

B) 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?

Click here to enter text.

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 HM Revenue and Customs).	☐

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?

Health & Social Care Act (Safety and Quality) Act 2015 – Direct Care Provision

The legal basis for commissioning purposes:

Power to commission certain health services – Power – Section 3A NHS Act 2006:

Each ICB has the power to arrange for the provision of such services or facilities as it considers appropriate for the purposes of the health service that relate to securing improvement in –

(a) the physical and mental health of persons for whom it has responsibility; or

(b) the prevention, diagnosis and treatment of illness in those persons.

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 SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT.	**Tick or leave blank** ☐

(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 i). 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
Buckinghamshire, Oxfordshire and Berkshire West ICB	Controller
Ufonia	Processor

1.5.

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

WHAT: Information provided by the referrer and patient demographic information obtained via other sources such as the national Personal Demographics Service e.g. referral letter and some structured data
WHY: to conduct autonomous telephone calls and / or electronic communications to patients referred to the single point of access
WHO: Staff working at Ufonia
Data to be processed is detailed in 2.3

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 records

1.7.

How are you satisfying the common law duty of confidentiality?
Reasonable expectations

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

The patient would reasonably expect their data to be shared, as it has been agreed at the point consent for referral is obtained.

1.8.

Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?
No – patient data cannot be anonymised as the patient has to be identified to ensure conversations with the correct patient on the correct pathway, and to keep the patient record up to date and accurate.
Confidentiality is preserved as the data is encrypted at rest, with 2 factor authentication, password protection and access limited to core members of staff. The data is not held in any physical form.

If you are, then describe what you are doing.
Click here to enter text.

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

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.

Yes - anonymised data will be used for reporting, analysing and evaluation purposes which does not relate to direct patient care. To give context: we use it for the Monthly BOB eMeet progress, we collect PROMS which are anonymised as well. The amalgamated anonymised data will be used as part of the service evaluation.

1.10.

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

~6,000 patients for the initial period of the project. Thereafter we anticipate ~15,000 per annum

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 e-mail
By SMS
Electronic (e-Referral Service - eRS)
Electronic (Rego)
By telephone, including automated calls
Paper form

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?

The data will be extracted from the referral documentation and formatted to enable upload to the Ufonia Dora platform for the purpose of making calls. In the case of missing data, other sources will be used to create a complete data set e.g. PDS.

Data will be edited by members of the Ufonia team to enable the service delivery to be carried out e.g. additional characters in telephone number will be removed (e.g. 07000 123456 Preferred will become 07000 123456)

1.13.

How will you quality check the data?

Referrers will ensure the data is accurate when sending to Ufonia. In this way, data quality will be assured through existing referral team processes. In addition, PDS may be used to validate the data and/or ensure complete data is available to deliver the service.

1.14.

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

Ufonia has a Business Continuity Plan and Incident Management Procedure which is tested on an annual basis, and stored on Ufonia's Quality Management System.

If yes include in the risk section of this template.

1.15.

What training is planned to support this activity?

- All members of Ufonia's team who are granted access to develop and deliver the system have contractual obligations to adhere to its quality management and information governance systems, including the completion of statutory and mandatory training in information governance that is consistent with the NHS DSPT.

- The Ufonia team operating the SPoA will be given training on how to use the Rego system, e-Referral system (eRS), secure email systems & Dora platform. This training will include how to carry out the procedures in the service specification, access policy and standard operating procedures relevant to this service.
- Training, onboarding, and familiarisation will be carried out with the referrers using a variety of mediums. In addition, Ufonia team members will be available to support specific queries from referrers to support service delivery.

2. LINKAGE, DATA FLOWS, SHARING AND DATA OPT OUT, SHARING AGREEMENTS, REPORTS, NHS DIGITAL

2.1.

Are you proposing to combine any data sets?

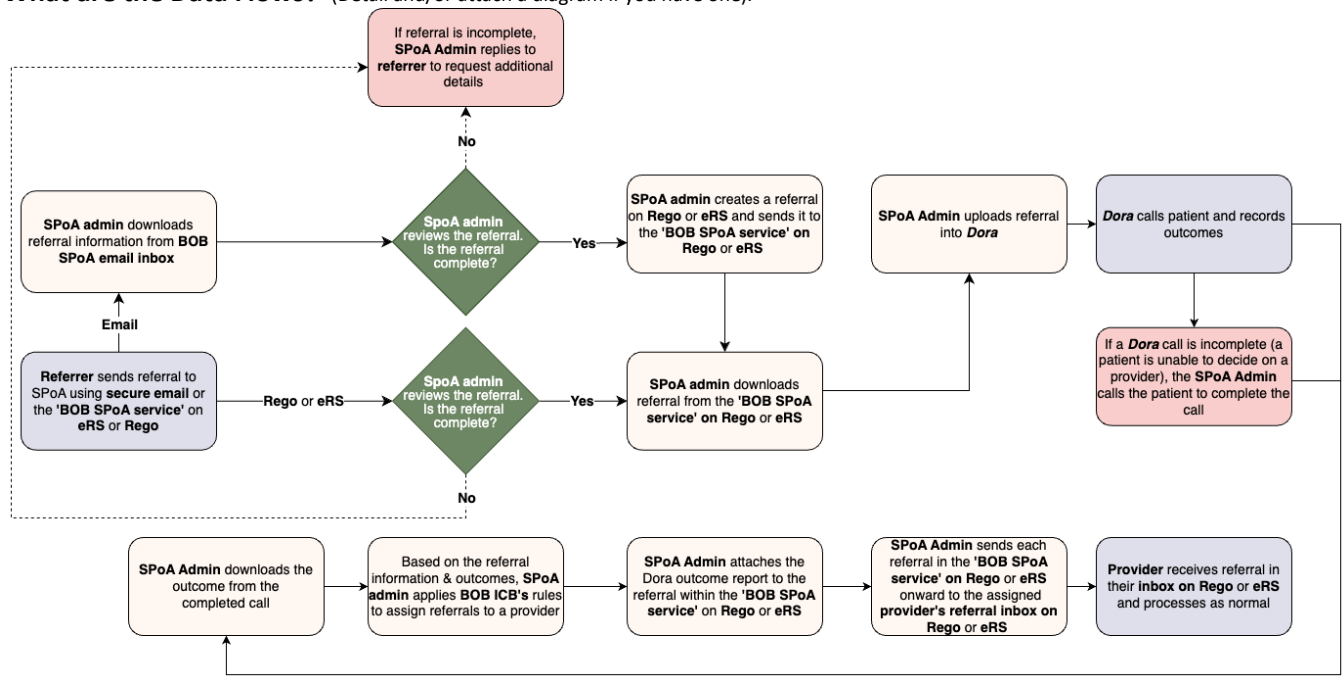
Yes

If yes then provide the details here.

We will be combining the referral information alongside PDS.

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?

Title/prefix/salutation

Desired to enable the system to greet the patient with the appropriate salutation

Forename & Surname

Required to enable the system to greet the patient by name and to check identity

Date of birth

Required to enable the system to conduct an identity check before progressing conversations

NHS number

Unique identifier

Required to retrieve data / enable the system to ensure patient data is accurate

Telephone number(s)
Required to enable the system to contact the patient to have routine clinical conversations

Specialty/Clinic/Condition
Required to enable the system to allocate the correct clinical conversation

Clinical symptoms/Clinical conditions
Required to assess patient eligibility to continue in the pathway

Post code
Required for the system to assess the distance from patient residence to potential providers

Additional information provided as part of the referral about the patient's condition (e.g. complex) and eligibility for a Dora call (e.g. deafness, cognitive impairment, non-English speaking)

Patient's preferred provider
Required to guide where referral is sent onward to

2.4.
Is any of the data subject to the National Data Opt Out?
No

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?
Provider organisations across the BOB ICS including NHS Trusts and the Independent Sector

2.6.
Why is this data/information being shared?
To enable the services to carry out triage, contact and care for patients on pathways

2.7.
How will you share it? (Consider and detail all means of sharing)
via electronic referral systems used by the provider organisations including but not limited to the national e-Referral Service (eRS) and/or Rego

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?
Not applicable.

2.9.
What reports will be generated from this data/information?
A report following the Dora call will be produced for the purposes of onward care along the patient's

pathway. This report, along with the original referral from the optometrist or GP will be sent onwards to the respective provider.

Anonymised summary reports will also be generated for the ICB to understand referral volumes, distribution, and patterns.

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
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.

C) 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.

Ufonia Ltd,
104 Gloucester Green,
Oxford,
OX1 2BU

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
Ufonia Ltd,	Yes	ZA563562
BOB ICB	Yes	ZB343068

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
Ufonia Ltd	This project will be covered through a contract between BOB ICB and Ufonia which includes the standard NHS Ts and Cs. A Data Processing Agreement will also be signed between BOB ICB and Ufonia. The following detail is taken from the Ufonia DPIA: Data Security and Protection Toolkit (DSPT) compliance • Organisation code: 8KH36

	Registered with the Information Commissioner's Office (ICO) • ZA563562 **On-Line DPA Register Search** Digital Technology Assessment Criteria (DTAC) assessment • See page here: Stated accreditations • Penetration Test Executive Summary available as pdf upon request Cyber Essentials or other cyber security certifications • **BM Registry | Ufonia Limited** • **BM Registry | f27b0389-fabb-410d-a52e-db736302dea2** • SPoA - BOB SPoA EIA V1.2 (BOB ICB).docx

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
Ufonia	8KH36	Standards Exceeded	27 June 2023
BOB ICB	**QU9**	Standards Exceeded	27 June 2023

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).

Information is stored in Amazon Web Services (AWS) and Google Cloud Platform (GCP) cloud-based systems, within the EEA.

Compliance frameworks:

https://cloud.google.com/security/compliance/compliance-reports-manager
https://aws.amazon.com/compliance/programs/

Security measures:

In transit:

Dora uses SSL (>= TLS 1.2) for data in transit between the application and end users, and between the application and sub-processors.

At rest:

Databases are encrypted using AES-256 or better.
Backups are encrypted at rest.
Network protection (including firewalls) applies to stored data.
A small number of key employees have access to production accounts.

All employee access requires multi-factor authentication.
Cloud providers handle physical security arrangements for the cloud resources.

3.6
How is the data/information accessed and how will this be controlled?

Ufonia staff will have access to the data for the purposes of ensuring and assuring the Dora calls accurately executed. This covers members of the operations, clinical, and product teams. All Ufonia staff have up-to-date mandatory data security and protection training (compliant with NHS DSPT).

When data is accessed, a record is made of the user, the request, and the timestamp.

The data is encrypted at rest, with 2 factor authentication, password protection and access limited to core members of staff. The data is not held in any physical form.

3.7
Is there any use of Cloud technology?
Yes

If yes, add the details here.
Data is stored on Amazon Web Servers (AWS) and Google cloud-based systems - within the EEA

3.8
What security measures will be in place to protect the data/information?

The following points are extracts from the Envisage DPIA

Encryption, password protection, role-based access controls, restricted physical access

- The data is encrypted at rest, with 2 factor authentication, password protection and access limited to core members of staff. The data is not held in any physical form.

Business continuity plans

- Ufonia has a Business Continuity Plan which is tested on an annual basis. This is backed up by Incident Management procedures. All are stored on Ufonia's Quality Management System.

Security policies

- All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

Others

- The system (Dora) is developed under a quality management system in line with IEC 62304 (software development lifecycle processes for medical devices).
- A UKCA (previously CE) mark for software-as-a-medical device has been awarded by the MHRA for the product and ongoing compliance with this standard will be maintained.

Ufonia has Data Protection Risk Register: https://ufonia.atlassian.net/wiki/spaces/UDFC/pages/5071798285

Ufonia have a number of security accreditations
- DSP Toolkit: Organisation code: 8KH36
- Cyber Essentials Plus: https://registry.blockmarktech.com/organisations/GBLTD10692039/

- CREST certified penetration test undertaken November 2023. Executive summary available on request

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)
Yes - outside the EEA
If yes, describe where and what additional measures are or will be in place to protect the data.

"Transfer" between the patient and Dora is over a phone call. All traffic between Dora and external service providers (e.g. speech to text) is done using TLS (wss and https). Admin portals use wss and https. Data storage and backups are within the same AWS region and managed by AWS.

Encryption is in place for data in transit via HTTPS.
For the EEA (and UK) we have agreements with all subprocessors that they do not retain any patient data.
A sub-processor ("Deepgram") is used to transcribe audio in real time with a data centre in the US (West and Midwest region). Ufonia has a Data Processing Agreement in place with the sub-processor and data is NOT retained for training their models (binary audio from the call is processed). The following are in place with Deepgram: Data Processing Agreement, Transfer Risk Assessment, International Data Transfer Assessment, Standard Contractual Clauses and UK Addendum.

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 will be in place between Ufonia and BOB ICB.

D) 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).
The ICB will include a note about Ufonia in its 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).

Information Rights Requests remain responsibility of the ICB as the data controller.

4.3
How long is the data/information to be retained?

BOB ICB will retain the data in line with the records management code of practice 2021. Ufonia will comply with ICB retention policies.

4.4
How will the data/information be archived?

No data will be archived as a result of this activity.

4.5

What is the process for the destruction of records?

Ufonia will securely destroy any sensitive data in line with trust and ICB retention policies and according to NHS best practice (consulting the SIRO as required).

4.6

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

This will be determined on a case-by-case basis with mutual agreement from the ICB and Ufonia (consulting the SIRO as required).

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.

E) 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. JB to review

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**
Errors or omissions in data received could result in delays to onward referral	Possible	Minimal	Low
Errors or omissions in data shared onward to provider could result in providers having to seek clarification from SPoA or recollect certain data from patient	Possible	Minimal	Low
Data breach could result in patient data being exposed	Remote	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)**
Errors or omissions in data received	Operational procedures to validate completeness of data, and seek clarification from the referrer as needed using Rego and/or eRS. Referral creation step on	Reduced	Low	Choose an item.

	eRS requires lookup on Patient Demographic Service, which would validate demographic information given.			
Errors or omissions in data shared onward to provider	Operational procedures to validate completeness of information and to match patient identifiers before referral sent onwards. Dora platform mandates input of required data fields.	Reduced	Low	Choose an item.
Data breach	Refer to measures in section 3	Reduced	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.

F) 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.

G) 7. DATA PROTECTION OFFICER COMMENTS AND OBSERVATIONS

7.1 Comments/observations/specific issues	Click here to enter text.

H) 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: Data Protection Officer

Signature: [redacted] Date: 30/04/2024

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.