NHS
Buckinghamshire, Oxfordshire and Berkshire West
Integrated Care Board

Ref: 23-24-025

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 :	31/01/2024
Title of the activity/processing:	Oviva Diabetes Support
Who is the person leading this work?	[redacted] – Diabetes Network Manager
Who is the Lead Organisation?	Oviva
Who has prepared this DPIA?	[redacted] – Long Term Conditions Project Manager
Who is your Data Protection Officer (DPO)?	[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).	Oviva have been commissioned by NHS Buckinghamshire, Oxfordshire and Berkshire West ICB to provide Oviva Diabetes Support (a remote Diabetes Structured Education service) to 833 patients with Type 2 diabetes over 12 months across Buckinghamshire, Oxfordshire and Berkshire West ICB with the option to extend the contract in line with the NHS Standard Contract. This DPIA relates to the Oviva Diabetes Support for Buckinghamshire, Oxfordshire and Berkshire West ICB. Oviva Diabetes Support is a remote type 2 diabetes structured education and behaviour change programme, delivered 1-to-1 by a diabetes specialist coach over 12 weeks. The programme includes support either over the phone or via a mobile app and access to Oviva's online portal which contains videos, podcasts and learning resources. Referral data will be provided from GP practices, Be Healthy Bucks (for Buckinghamshire only) or secondary care trust as well as through the self referral portal provided by Oviva. This referral form will be used for patients identified as suitable for the provider service and passed to the provider, Oviva, using NHS email. This will allow Oviva to contact the patient. Patient data will also be shared back with the patient's practice in order to code whether the individual has attended/completed. This also, will be via secure nhs.net email address.
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, Oviva UK, GP Practices, Be Healthy Bucks, Oxford Health Foundation Trust
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?	This programme has been running in Buckinghamshire since 2018. We are now extending the service to cover Oxfordshire and Berkshire West as well.

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 (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).	**Tick or leave blank**
	☐

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 (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).	**Tick or leave blank**
	☐

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 (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).	**Tick or leave blank**
	☐

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). **Health & Social Care Act 2012 Sec3 (a) requires each integrated care board 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—** **(a)in the physical and mental health of the people for whom it has responsibility, or** **(b)in the prevention, diagnosis and treatment of illness in those people.**	**Tick or leave blank** ✓
What statutory power or duty does the Controller derive their official authority from?	
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. (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 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**
Referring GP Practices – Data Controller	Sole Controller
Oviva UK Limited – Data controller for care delivered after receiving referrals via NHSmail	Sole Controller
Be Healthy Bucks (Maximus UK) – Data Controller (Buckinghamshire Single Point of Access)	Sole Controller
Buckinghamshire, Oxfordshire & Berkshire West ICB - Commissioner	Other
Oxford Health Foundation Trust	Sole Controller
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 data will be used to provide patient care through Oviva Diabetes Support.

Data items that are held in system:

Personal

x Name
x Address
x Post Code
x Date of Birth
x GP Practice
x NHS Number

Special Categories
x Health Data
x Racial or Ethnic Origin

At the end of the programme, patients will be discharged back to their GP practices via a discharge summary sent via NHSmail. This summary will include the relevant SNOMED codes to be entered into the GP system.

In order to report on the service against contractual requirements, Oviva will share an anonymous consolidated dataset with Buckinghamshire, Oxfordshire and Berkshire West ICB. This dataset will include the service activity including number of referrals, number of participants completing the programme, NHS Friends and Family Test, changes in self-confidence in managing diabetes compared to baseline, etc.

Patients will be referred into the Oviva Diabetes Support service by the referrer, by submitting a referral form via secure NHSmail. Patients will also be able to self-refer in through the Oviva website page - https://oviva.com/uk/en/programmes/diabetes-support/#form

For Buckinghamshire, referrals are received via the Be Healthy Bucks (single point of access) hub. Patients are referred in to the Oviva Diabetes Support service by the Be Healthy Bucks hub, by submitting a referral form via secure NHSmail.

The data collected is being used to deliver Oviva Diabetes Support, a Diabetes Structured Education programme delivered over 3 months. During this time more data is collected about the patient as they track their progress through the programme. This is collected via Oviva's coaches and stored on the patient's medical record within OCS.

Patients will add to the dataset by self-monitoring their progress against the goals set with their coach via the Oviva app.

Oviva's coaches will add to the dataset by documenting clinical notes in Oviva's secure electronic medical record following patient coaching appointments.

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?
Consent - Implied

If you have selected an option which asks for further information please enter it here
Click here to enter text.

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.
Business Intelligence will conduct this for NHS Reporting.

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.

Click here to enter text.

1.10.

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

500 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.

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?

The data collected is used to deliver Oviva Diabetes Support, a Diabetes Structured Education programme delivered over 3 months. During this time more data is collected about the patient as they track their progress through the programme. This is collected via Oviva's coaches and stored on the patient's medical record within OCS.

1.13.

How will you quality check the data?

All information will be quality checked by Oviva and the GP practice at all interactions with the patient.

Accuracy of patient data is very important at Oviva. Staff Information Governance training is regularly carried out to reiterate the importance of preserving the accuracy of data records and checks are carried out to ensure data anomalies are identified, i.e. inaccurate weight measurements are identified through a regular data review conducted by Oviva's data analytics team. Patients can at any time request for a perceived data inaccuracy to be reviewed and amended if required. The process for doing this is laid out in Oviva's Privacy Policy, which is made available at all times to Oviva's patients.

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?

No additional training is identified to support this activity.

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

2.1.

Are you proposing to combine any data sets?

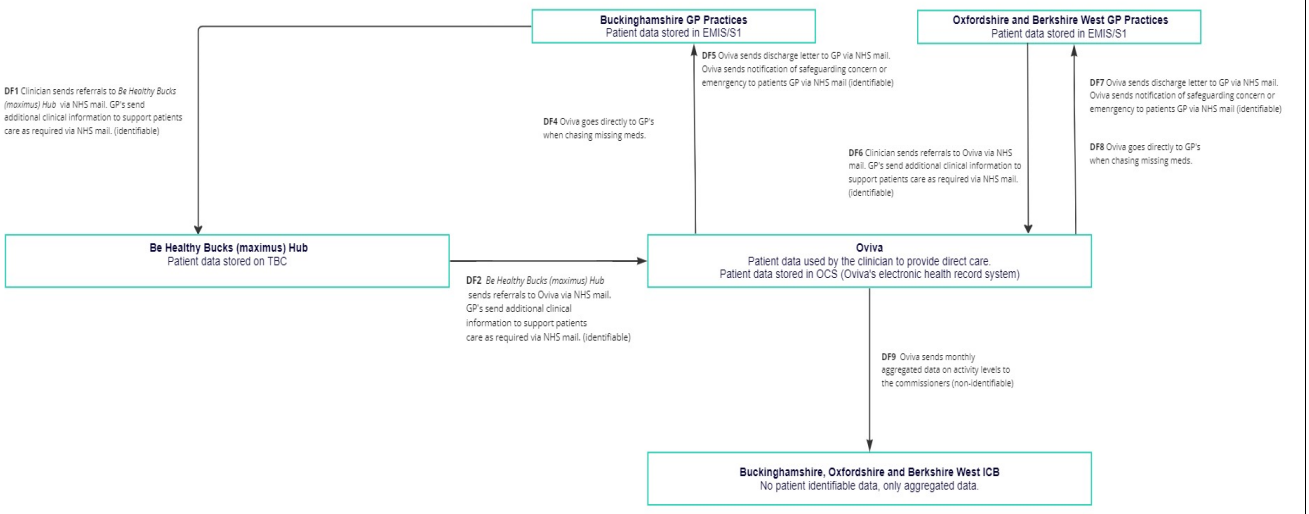
Yes

If yes then provide the details here.

Oviva will be combining Oxon and Bucks data sets and sharing with the ICB (KPI aggregated data that we share monthly)

2.2.

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



Oviva is providing clinical care to patients in Buckinghamshire, Oxfordshire and Berkshire West and personal data will be collected and shared about a patient, where necessary to support their clinical care.

All patients will agree to be referred to Oviva, no referral will be sent to Oviva without the referrer (GP, Oxford Health FT or hub) informing the patient.

Patients will be referred into the Oviva Diabetes Support service by the referrer by submitting a referral form via secure NHSmail. The data collected as part of this service relates only to patients referred into this service.

Patients can add to the dataset by self-monitoring their progress against the goals set with their coach via the Oviva app. Oviva's coaches will add to the dataset by documenting clinical notes in Oviva's secure electronic medical record following patient coaching appointments.

Once Oviva receives a referral, all data will be added to and stored on Oviva's secure electronic medical record - called the Oviva Coaching Suite (OCS). Oviva also uses Google Cloud Platform (offered by Google Cloud EMEA Ltd, 70 Sir John Rogerson's Quay, Dublin 2, Ireland) to host the patient data, on servers hosted in Germany.

The data collected is used to deliver Oviva Diabetes Support, a Diabetes Structured Education programme delivered over 3 months. During this time more data is collected about the patient as they track their progress through the programme. This is collected via Oviva's coaches and stored on the patient's medical record within OCS. All information will be quality checked by Oviva and the GPs, Homerton Diabetes Service and Community Care Team at all interactions with the patient.

At the end of the programme, patients will be discharged back to their GP practices via a discharge summary sent via NHSmail. This summary will include the relevant SNOMED codes to be entered into the GP system.

To report on the service against contractual requirements, Oviva will share an anonymous consolidated dataset with Buckinghamshire, Oxfordshire and Berkshire West ICB . This dataset will include the service activity including number of referrals, number of participants completing the programme, NHS Friends and Family Test, changes in self-confidence in managing diabetes compared to baseline, etc. Oviva will report back to the commissioner monthly via an Excel KPI report, containing aggregated data on activity levels.

Support provided to patients following their first appointment varies, but will consist of weekly support, provision of a coach and regular updates. Patients can choose to interact with the service through an App. If they do not wish to download the App, they will be provided with weekly telephone support and be provided with all relevant information and guidance this way.

2.3.
What data/information are you planning to share?
PID will not be received by the ICB. Performance data/numbers of patients will be shared with the ICB.

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?
Information is only shared between Oviva and the patient. Oviva will share numbers of patients/performance data with the ICB but no patient metrics/identifiable information.

2.6.
Why is this data/information being shared?
For patient treatment and information shared with the ICB is for monitoring purposes.

2.7.
How will you share it? (Consider and detail all means of sharing)
Electronically via secure email

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?

Data Sharing Agreement not required for direct care.

2.9.
What reports will be generated from this data/information?

Performance reports which include the number for patients seen each month within the service, provided to the ICB for monitoring purposes.

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.

Google Cloud
70 Sir John Rogersons Quay
Dublin
Dublin 2
Oviva UK
Runway East
20 St. Thomas St.
London
SE1 9RS

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
Google Cloud	Yes	Registration Certificate Google C ZB182706
Oviva	Yes	Registration Certificate Oviva UK ZA253788

Oxford Health Foundation Trust	Yes	Registration Certificate Oxford N Z1411013
Be Healthy Bucks (Maximus UK)	Yes	ZA103012
Bucks GP Practices	Yes	Bucks GP DSPT & ICO.xlsx
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
Google Cloud	Compliance assurance includes: Cyber Essentials Plus certification obtained NHS Digital: Digital Assessment Questionnaire certification obtained ICO Registration obtained
Oviva UK Limited	Oviva is Cyber Essentials accredited (last accredited July 2022) and Cyber Essentials Plus accredited (latest being September 2022) and conducts regular external accredited penetration testing (last tested July 2022). No findings or major risks were reported from the last penetration test. Oviva is ISO 27001 certified by an external independent certified body. ISO 27001 certification is proof that Oviva have a robust information security management system, including system level security policies.
Oxford Health Foundation Trust	DSPT toolkit
Be Healthy Bucks (Maximus UK)	DSPT Toolkit
Bucks GP Practices	DSPT Toolkit
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
Oviva UK Limited	8JE35	Exceeding Standards	01/03/2023
Oxford Health Foundation Trust	RNU	Standards Met	30/06/2023
Be Healthy Bucks (Maximus UK)	8KH29	Standards exceeded	26/06/23
Bucks GP Practices	Click here to enter text.	Click here to enter text.	Bucks GP DSPT & ICO.xlsx
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).

Once Oviva receives a referral, all data will be added to and stored on Oviva's secure electronic medical record - called the Oviva Coaching Suite (OCS).

Oviva use Google Cloud Platform to host the data. The data is processed on servers in Germany. Google is an international organisation which is why we have a processing contract with Google, including EU standard contractual clauses, according to which Google undertakes to comply with European data protection, in order to guarantee a level of data protection that corresponds to that of the UK and EU.

3.6

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

Oviva's secure electronic medical record where the data will be held has secure user access controls in place and two step user authentications established.

Access to patient data within Oviva's electronic medical record 'OCS' is limited to those who need access to deliver the Oviva Diabetes Support service:

- Healthcare professionals employed by Oviva to deliver this service
- Oviva's Patient Pathway Coordinator team to support patients during their time on the programme, i.e. book appointments, amend appointments
- Oviva's analytics team in order to monitor the accuracy of data entered and generate reporting required to deliver the service, i.e. the monthly KPI report
- Oviva's Service Delivery Lead assigned to manage the service in order to support delivery

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

We use Google Cloud Platform to host the data. The data is processed on servers in Germany. Google is an international organisation which is why we have a processing contract with Google, including EU standard contractual clauses, according to which Google undertakes to comply with European data protection, in order to guarantee a level of data protection that corresponds to that of the UK and EU.

3.8

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

Section 6.1G of Oviva's Data Privacy Manual sets out how Oviva provide security for patient data to ensure personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage:

6.1g: Availability control

It must be ensured that personal data is protected against accidental destruction or loss.

Measures adopted by the Oviva staff:

- *Testing the recovery*

Measures adopted in the data centre:

- *Backup systems to recover lost data*
- *UPS (uninterruptible power supply)*
- *Redundant power supply*
- *Emergency generator*

- *Fire alarm*
- *Fire protection and disaster recovery plan*
- *Documented data protection concept*
- *Centralised data backup*
- *Physically separate storage of the generated backup*
- *Object security especially the server rooms*
- *Air conditioning*
- *Anti-malware concept (SE Linux, OSSEC and ClamAV)*

Oviva is Cyber Essentials accredited (last accredited July 2022) and Cyber Essentials Plus accredited (latest being September 2022) and conducts regular external accredited penetration testing (last tested July 2022). No findings or major risks were reported from the last penetration test.

Measures that Oviva takes to protect against damage to data are:

• Access controls are in place to ensure only the correct individuals have access to the data, i.e. users are authenticated via SSH keys and VPN certificates, all administrators are required to use multi-factor authentication. Access is controlled on multiple levels from host based down to database table based. Depending on the access level of users we use suitable authentication methods to protect access to the data, i.e. either password, password and TOTP, password and smart key, or TOTP, password and key files
• Data is hosted via Google Cloud Platform to host the data. Data is processed on servers in Germany. Google is an international organisation which is why we have a processing contract with Google, including EU standard contractual clauses, according to which Google undertakes to comply with European data protection, in order to guarantee a level of data protection that corresponds to that of the UK and EU.
• All data in transit from clients to servers is encrypted with TLS 1.2, only strong ciphersuites are permitted
•Servers are walled off by a dedicated firewall and access is only permitted via VPN and SSH, authentication is key based

Accuracy of patient data is very important at Oviva. Staff Information Governance training is regularly carried out to reiterate the importance of preserving the accuracy of data records and checks are carried out to ensure data anomalies are identified, i.e. inaccurate weight measurements are identified through a regular data review conducted by Oviva's data analytics team.

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.

Oviva is ISO 27001 certified by an external independent certified body. ISO 27001 certification is proof that Oviva have a robust information security management system, including system level security policies.

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.
We use Google Cloud Platform to host the data. The data is processed on servers in Germany. Google is an international organisation which is why we have a processing contract with Google, including EU standard

contractual clauses, according to which Google undertakes to comply with European data protection, in order to guarantee a level of data protection that corresponds to that of the UK and EU.

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?

Oviva holds a data processing agreement with Google Cloud.

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).

No proposed changes. Referral to providers included within the current GP FPN and Oviva has its own Privacy Notice available here: https://oviva.com/uk/en/legal/#privacy

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).

Staff Information Governance training is regularly carried out to ensure all Oviva staff understand how to deal with a Subject Access Request (SAR). All requests are referred to Oviva's Data Protection Officer, who is trained in how to appropriately handle a SAR. Patients are informed of how to make a SAR via Oviva's Privacy Policy, which is made available to all Oviva patients at the point of enrolment onto Oviva Diabetes Support and can be found on Oviva's website.

All SARs are reviewed individually and dealt with in accordance with the DPA 2018. All requests are processed within 30 days of being filed. All data held by Oviva can be retrieved from the Oviva Coaching Suite and provided to the patient securely via NHSmail. As patients do not have NHSmail the files will be sent using the [secure] tag in the subject line to ensure the message is encrypted when it is sent to a non-NHSmail email address. Patients are made aware of how they can contact Oviva with any queries or further requests.

Data subjects initiates a request to Oviva UK Limited for a copy of their data by emailing privacy@oviva.com. Oviva UK Limited then verifies the identity of the data subject.
All data held by Oviva can be retrieved from the Oviva Coaching Suite and provided to the patient securely via NHSmail. As patients do not have NHSmail the files will be sent using the [secure] tag in the subject line to ensure the message is encrypted when it is sent to a non-NHSmail email address. Patients are made aware of how they can contact Oviva with any queries or further requests.

All data controllers are responsible for managing Individual rights requests in line with their policies and procedures.

4.3

How long is the data/information to be retained?

As per the guidance from NHS England on the retention periods for adult health care records, Oviva store patient data for 8 years after the last interaction with the patient.

After this time point the patient data is permanently deleted so long as Oviva are not required to hold it for legal reasons. This information is included in Oviva's Privacy Statement.

4.4

How will the data/information be archived?

As per the guidance from NHS England on the retention periods for adult health care records, Oviva store patient data for 8 years after the last interaction with the patient.

After this time point the patient data is permanently deleted so long as Oviva are not required to hold it for legal reasons. This information is included in Oviva's Privacy Statement.

4.5

What is the process for the destruction of records?

Oviva has a BigQuery stored procedure that takes a list of patient ids as input, and it removes all associated PII fields from all database tables for those patients. The stored procedure is written in standard SQL (DELETE entire rows, UPDATE to overwrite PII fields with blanks). Google manages the backups for BigQuery and they guarantee that all copies of customer deleted data will be permanently removed from all their systems within max 180 days of the request: **https://cloud.google.com/docs/security/deletion#deletion_timeline**

4.6

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

It will be stored only in accordance with applicable (data retention) law(s) and then deleted pursuant to any and all applicable agreement(s).

If for any reason Oviva were to go out of business, the managing of data would depend on whether the business is sold via share or asset. The NHS Contract would be followed and if the business were to dissolve/become bankrupt, then the data would be returned to the sender.

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**
Risk to patients – referral data is sent by the referrer to an email that is not Oviva's NHSmail address.	Possible	Minimal	Medium
Risk to patients – data is sent by Oviva to referrer on a non NHSmail email address.	Possible	Minimal	Medium

Data breach such as unauthorised access to systems or data	Possible	Significant	Medium
Data kept for longer than retention period	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)**
Risk to patients – referral data is sent by the referrer to an email that is not Oviva's NHSmail address.	Oviva continues to provide training briefings to staff highlighting the importance of taking care when receiving patient data and highlighting errors made.	Reduced	Low	Choose an item.
Risk to patients – data is sent by Oviva to referrer on a non NHSmail email address.	As above. Oviva have confirmed they have appropriate IG training in place for staff.	Reduced	Low	Choose an item.
Data breach such as unauthorised access to systems or data	Password policy, staff training and awareness, access control, secure hosting and data minimised to what is necessary. Oviva is Cyber Essentials Plus accredited (latest being September 2022) and conducts regular external accredited penetration testing (last tested June2022). No findings or risks were reported from the last penetration test. Access controls are in place to ensure only the correct individuals have access to the data, i.e. users are authenticated via SSH keys and VPN certificates, all	Reduced	Low	Choose an item.

	administrators are required to use multi-factor authentication. Access is controlled on multiple levels from host based down to database table based. Depending on the access level of users we use suitable authentication methods to protect access to the data, i.e. either password, password and TOTP, password and smartkey, or TOTP, password and keyfiles			
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

5.3
What if anything would affect this piece of work?
None

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?
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 For BOB GP Practices [Comments added Monday 24 June 2024]: The GP Practices should read and fully understand this DPIA, and the risks set out in section 5. • The GP Practices should understand the mitigations required and action as appropriate to reduce risks where possible set out in section 5.2 of this DPIA. • The GP Practices should update their Information Asset Register and Data Flow Map to reflect this process.

	The GP Practices should update their Privacy Notice to reflect this process. Suggested wording RECOMMENDATION: Purpose: Oviva have been commissioned by NHS Buckinghamshire, Oxfordshire and Berkshire West ICB to provide Oviva Diabetes Support (a remote Diabetes Structured Education service). Oviva is providing clinical care to patients in Buckinghamshire, Oxfordshire and Berkshire West and personal data will be collected and shared about a patient, where necessary to support their clinical care. Referral data will be provided from GP practices, Be Healthy Bucks (for Buckinghamshire only) or secondary care trust as well as through the self referral portal provided by Oviva. Patients will be informed before being referred to Oviva, no referral will be sent to Oviva without the referrer (GP, Oxford Health FT or hub)informing the patient. Legal Basis of Processing: Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…' Article 9(2)(h) '… the provision of health or social care or treatment of management of health or social care systems…' BOB ICB DPO 24/06/2024: The comments made and advice given by the GP DPO are supported recommended to GP practices.

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: 24/06/2024

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

Name: Click here to enter text.

Job Title: Click here to enter text.

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

Please note:

You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant as a result of this project.

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.