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 :	08/06/2023
Title of the activity/processing:	NHS Type 2 Transmission to Diabetes Remission Programme
Who is the person leading this work?	[redacted] (BOB ICS)
Who is the Lead Organisation?	Oviva UK Ltd
Who has prepared this DPIA?	[redacted] (Oviva Mobilisation Manager) & [redacted] (Oviva Governance Lead)
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).	The NHS Type 2 Diabetes Path to Remission is a service for people with type 2 diabetes. It is a one-year programme to support healthier lifestyle, weight loss and remission of Type 2 diabetes. The programme consists of nutritionally complete total diet replacement products, for 12 weeks, followed by a period of food reintroduction and subsequent weight maintenance support, with a total duration of 12 months. The programme is delivered by Oviva, for any eligible patients referred by GPs in the eligible areas. The contract for the provision of the programme is held between NHSE and Oviva, with data flowing between Oviva and GP surgeries directly and between Oviva and the commissioners for reporting. Data is also provided to Buckinghamshire, Oxfordshire & Berkshire West ICB (only in aggregate form) to enable monitoring of referrals and ensure the overall success of the programme. This programme is available for all Buckinghamshire, Oxfordshire & Berkshire West residents who meet the eligibility criteria for the programme.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	The programme is delivered by Oviva UK Ltd, for any eligible patients referred by GPs in the eligible areas. Oviva UK Limited will be a data controller (after receiving referrals from GP practices) for the programme. The contract for the provision of the programme is held between NHSE and Oviva UK Ltd, with data flowing between Oviva UK Ltd and GP surgeries directly and between Oviva and the commissioners for reporting. Data is also provided to the ICB (only in aggregate form) to enable them to monitor the referrals and ensure the overall success of the programme.
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	NHS England
Detail anything similar that has been undertaken before?	Oviva UK Ltd previously provided Low Calorie Diet (LCD) Pilot across several areas and currently holds 9 T2DR contracts (Type 2 Diabetes Path to Remission contracts).

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:

c) THE DATA SUBJECT HAS GIVEN CONSENT	**Tick or leave blank**
	✓

Why are you relying on consent from the data subject?

The patient is required to give their consent at the point of referral, for their personal data to be shared with Oviva UK Ltd. so that they can participate in the NHS Type 2 Diabetes Pathway to Remission Programme of which Oviva UK Ltd are the new provider.

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

Referrals to the Programme will be from GP practices. Individuals will be identified during their regular diabetes review or following a search of the clinical system. The individual's medical history will be considered in detail to ascertain their appropriateness for the programme and where they satisfy all the eligibility criteria, they may choose to be referred to the programme.

As a controller, the referrer is required to explain to the individual how their data will be used at the point it is collected from them – i.e. before referring them. This is referred to as a privacy notice. The process for referral to the programme is for local determination and will require dialogue with programme providers.

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

N/A

d) 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?

NHS Type 2 Diabetes Pathway to Remission Programme

e) 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.	
f) 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.	
g) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	**Tick or leave blank** ✓
What statutory power or duty does the Controller derive their official authority from? Health and Social Care Act 2012	
h) 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
Oviva UK Ltd	Data Controller
NHSE	Other
Buckinghamshire, Oxfordshire & Berkshire West ICB	Other
Buckinghamshire, Oxfordshire & Berkshire West GP Practices	Data Controller

1.5.

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

The following data is received from the individual's GP or other NHS representative. The GP sends a referral form which is on DXS and sent via DXS or by secure email directly to the provider when they are referred to the programme:

- Full name and title
- Postal address and postcode
- Phone number(s)
- Email address
- NHS Number
- Date of Birth
- Age
- Gender
- Ethnicity
- GP surgery (and from that ICB/contract)
- Weight (sensitive personal data)

- Height (sensitive personal data)
- BMI (sensitive personal data)
- HbA1c reading (sensitive personal data)
- Date of type 2 diabetes diagnosis
- Blood pressure medication and dosage (sensitive personal data)
- Diabetes medication and dosage (sensitive personal data)
- Other medication details and dosage (sensitive personal data)
- Blood glucose, blood pressure (sensitive personal data)
- Long-term health condition (sensitive personal data)
- Disability (sensitive personal data)
- Relevant past medical history/current comorbidities (sensitive personal data)

Once Oviva on boards a patient onto the service, all data will be added to and stored on Oviva's secure electronic medical record - called the Oviva Coaching Suite (OCS). We use Google Cloud Platform to host the data. Their 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.

Google Cloud is NHS compliant and please see more information via below link
NHS (UK) | Google Cloud

Referrals to the Programme will be from GP practices. Individuals will be identified during their regular diabetes review or following a search of the clinical system. The individual's medical history will be considered in detail to ascertain their appropriateness for the programme and where they satisfy all the eligibility criteria, they may choose to be referred to the programme.

As a data controller, the referrer is required to explain to the individual how their data will be used at the point it is collected from them – i.e., before referring them. This is referred to as a privacy notice. The process for referral to the programme is for local determination and will require dialogue with programme providers. The contract sets out the expectation that it is the responsibility of the provider to arrange attendance and provide further information to patients as controller of their personal data (e.g. privacy notice) for those individuals that have been referred. As a data controller, it is for individual GPs to determine the relevant lawful basis for the processing of any personal data as part of the programme. However, it is more likely than not that this will come under:

• UK GDPR Article 6(1)(e) [personal data] – …necessary for the performance of a task carried out in the public interest (a public task) or in the exercise of official authority…

• UK GDPR Article 9(2)(h) [special category data] - …necessary for the purposes of preventative or occupational medicine…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services…

When relying upon Article 6 (1) (e), a task carried in the exercise of official authority is derived from the relevant sections of the NHS Act 2006 as amended by the Health and Social Care Act 2012 where a Controller is providing a service commissioned under a duty stated in that act.

With reference to duty of confidence, as this relates to direct care and privacy information is provided prior to any processing of personal data that includes the quality of confidence the information will reside. A patient, in their discussions with their GP about this treatment, signalling agreement to the treatment either verbally

or in written format and further onward journey through treatment can be regarded as consent under common law duty of confidentiality.

The referral, with accompanying information (see section 6.1), must be communicated securely to the provider.

All data is stored and processed in Germany, but held in the UK or in the EEA via Google cloud based platforms. Google decides where the data is held, but it is not held outside the EEA. In the unlikely event that Google are required to send data outside of the EEA, Google will always ensure that we have adequate safeguards in place.

Oviva's secure electronic medical record where the data will be held has secure user access controls in place and two step user authentication established. Access to patient data within Oviva's electronic medical record 'OCS' is limited to those who need access to deliver the Oviva Adult ONS Medicines Management 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 Operations Manager assigned to manage the service in order to support delivery

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)
Health information

1.7.

How are you satisfying the common law duty of confidentiality?
Consent - Implied
Under the Common Law Duty of Confidentiality, information can be shared for the purposes of direct care with the reasonable expectation that the data subject understands their data will be shared.

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.
Anonymised reports to NHSE and to Buckinghamshire, Oxfordshire & Berkshire West ICB

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?
100+

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 - The data will be collected at the point of GP referral via NHSmail. The form is on DXS and can be sent through DXS, or emailed. The form must be completed in full - email referrals without the completed form are not accepted

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 securely and appropriately edited as and when changes in personal information occur (including sensitive data). This will be done via our OCS platform and completed by all relevant care delivery staff, with strict access control.

1.13.

How will you quality check the data?

Data provided by GPs in referrals follows a defined workflow involving numerous automated checks and human interventions. Furthermore, data is reverified with the patient during the onboarding call and subsequent interactions with Oviva UK Ltd to ensure it is accurate.

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?

Oviva has the relevant policies and procedures in place to ensure that Information Governance standards are adhered to and all employees complete mandatory Information Governance training with annual completion tracked by IG Lead. This is to reiterate the importance of the security of data records. The staff contracts also include relevant articles to ensure the staff compliance with completion of regular appropriate IG training in order to ensure data security being embedded within the organisation.

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

2.1.

Are you proposing to combine any data sets?

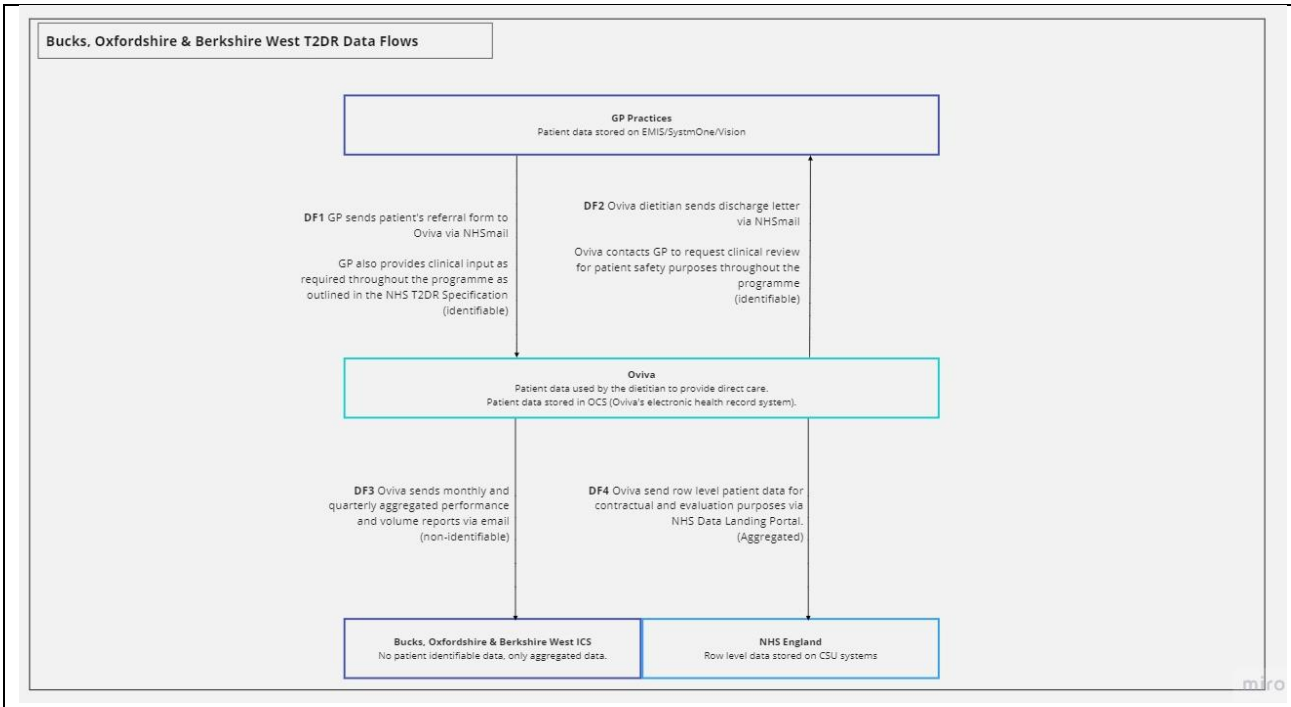
Not applicable

If yes then provide the details here.

Click here to enter text.

2.2.

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



Data Flow (DF in image) 1 is the transfer of patient identifiable information from BOB GP Practices to Oviva for the referral of the patient to the Oviva T2DR Programme, and any other clinical communication throughout the programme. All of this will be done via NHSmail.

DF2 is the transfer of patient identifiable data from Oviva back to BOB GP Practices for the discharge of patients and any clinical communication throughout the programme. All of this will be done via NHSmail.

DF3 is the transfer of non-identifiable, aggregated data from Oviva to the BOB ICS. This is aggregated monthly and quarterly reports with no patient identifiers.

DF4 is the monthly transfer of patient non-identifiable, aggregated low level data from Oviva to NHS England for contractual purposes via NHS Data Landing Portal.

Patient identifiable data will flow from GP practice to Oviva in a referral form, and Oviva will provide information back to the GP practice as a discharge letter from the service. During the service Oviva will periodically send the GP practice updates on the patient's progress to help inform medication change decisions made by the GP. All data transferred will be via NHS.net to ensure the transfer is secure.

2.3.

What data/information are you planning to share?

The following data is received from the individual's GP or other NHS representative when they are referred to the programme:

- Full name and title
- Postal address and postcode
- Phone number(s)
- Email address
- NHS Number
- Date of Birth
- Age
- Gender
- Ethnicity

- GP surgery (and from that ICB/contract)
- Weight (sensitive personal data)
- Height (sensitive personal data)
- BMI (sensitive personal data)
- HbA1c reading (sensitive personal data)
- Date of type 2 diabetes diagnosis
- Blood pressure medication and dosage (sensitive personal data)
- Diabetes medication and dosage (sensitive personal data)
- Other medication details and dosage (sensitive personal data)
- Blood glucose, blood pressure (sensitive personal data)
- Long-term health condition (sensitive personal data)
- Disability (sensitive personal data)
- Relevant past medical history/current comorbidities (sensitive personal data)

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?

Throughout the programme, we may share personal data with the below third parties:

- The patient's GP, so that they are aware of the patient's progress on the programme, can record relevant read codes on the patient's medical records, and can react appropriately to any health incidents or other concerns
- NHS England, who have commissioned the NHS Type 2 Diabetes Remission Programme, for the purposes of monitoring the success of the programme and managing invoicing and payment for the provision of the programme
- Third parties who provide operational services for us to deliver the contract and service (more details can be found via privacy policy. https://oviva.com/uk/en/standard-data-privacy/)
- Third parties to whom Oviva may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. *(Please be* assured that this point *is designed to capture notice for a situation where there is a transfer of parts of the business. There is nothing like that on this horizon at this point in time however as the patient may know, Biotech/health tech companies, and so forth, sometimes do transfer assets one between the other. This would incorporate patient data if this was to happen in the future, we would provide the patient with a notice that this was going to happen and offer the opportunity to exercise their subject access rights just to be able to redact the information and all the rest of it. However at this point in time, Oviva has no plans to sell part of or all of the business.)*

We require all third parties to respect the security of personal data and to treat it in accordance with data protection laws. Where we share personal data with third parties who provide operational services to us, we only permit them to process your personal data for specified purposes in accordance with our instructions.

2.6.
Why is this data/information being shared?

- Oviva have been commissioned by NHS England to provide NHS Type 2 Diabetes Remission Programme to patients registered with BOB GP Practices. To enable care delivery, it is necessary for BOB GP practices to share patients' data with Oviva when they are referred to Oviva and enrolled on T2DR Programme. The patient's GP, so that they are aware of the patient's progress on the programme, can record relevant read codes on the patient's medical records, and can react appropriately to any health incidents or other concerns
- As a part of contractual obligations, Oviva is obliged to send aggregated data to NHS England, who have commissioned the NHS Type 2 Diabetes Remission Programme, for the purposes of monitoring the success of the programme and managing invoicing and payment for the provision of the programme.
- There have been third parties that provide operational services for Oviva to deliver the contract and service (more details can be found via privacy policy. https://oviva.com/uk/en/standard-data-privacy/)
- Third parties to whom Oviva may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. *(Please be* assured that this point *is designed to capture notice for a situation where there is a transfer of parts of the business. There is nothing like that on this horizon at this point in time however as the patient may know, Biotech/health tech companies, and so forth, sometimes do transfer assets one between the other. This would incorporate patient data if this was to happen in the future, we would provide the patient with a notice that this was going to happen and offer the opportunity to exercise their subject access rights just to be able to redact the information and all the rest of it. However at this point in time, Oviva has no plans to sell part of or all of the business.)*

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?
A Data Sharing Agreement is in place between BOB GP Practices and Oviva UK Ltd to transfer patient data securely via NHSmail.

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

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.

I) 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 (for details go to 3.5)

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
Oviva UK Limited	Yes	ZA253788
BOB ICB	Yes	ZB343068
Google Cloud EMEA Limited	Yes	ZB182706
NHSE	Yes	Z2950066

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 EMEA Limited	There has been a processing contract between Oviva and 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. NHS (UK) | Google Cloud.

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 Ltd Please access details via below link: https://www.dsptoolkit.nhs.uk/OrganisationSearch/8JE35	8JE35	Standards Exceeded	01/03/2023
BOB ICB	QU09	Standards Exceeded	27/06/2023

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).

Once Oviva on boards a patient onto the service, all data will be added to and stored on Oviva's secure electronic medical record - called the Oviva Coaching Suite (OCS). We use Google Cloud Platform to host the data. Their 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.

Google Cloud is NHS compliant and please see more information via below link
NHS (UK) | Google Cloud

3.6

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

The OCS access controls are specified in Oviva's Data Privacy Manual section 6.1. For specific users the access controls are as follows:

Individual users access control: It is to be ensured that the persons entitled to use our data processing systems can only access the data subject to their access authorization, and that personal data cannot be read, copied, modified or removed during the processing, use and storage after unauthorised use.

Measures taken: identification and authentication of users; provide a differentiated authorization concept according to the need-to-know principle; automated verification of authorisations; introduction of restrictive measures (e.g. read only authorization); central distribution of user rights only after justified application.

We have security procedures in place to monitor access and identify inappropriate access. There have been appropriate controls implemented to generate security tickets for the security team to monitor and take actions accordingly.

We have an internal system to identify and monitor unauthorised access. Appropriate staff from security (security@oviva.com) and management team will be notified to investigate the matter and immediately mitigate risk arising.

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

Please see section 3.5 for more details.

3.8

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

All transfer of information from Oviva to GPs is via secure NHSmail.
All data in transit from clients to servers is encrypted with TLS 1.2, only strong cipher suites are permitted

Is a specific System Level Security Policy needed?

Yes

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.

We use Google Cloud Platform to host the data. Their 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.

Google Cloud is NHS compliant and please see more information via below link
NHS (UK) | Google Cloud.

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?

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.

J) 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).

Not applicable

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).

Each Controller is responsible for putting in place and applying effective procedures to address complaints about data sharing and requests from Data Subjects relating to this programme/project. This includes making provision for the Data Subject rights under GDPR articles 15, 16, 18, 21 and, DPA sections 45, 46, 47 and 99 rights of access, rectification, restriction and objection to sharing.

Oviva has internal procedures in place to provide access to records. The data subjects can make a Subject Access Request (SAR) to access personal data (e.g. call recordings) with a copy of their identification (passport, driving licence) by mail to Oviva UK Limited, Runway East, 20 St Thomas Street, London, SE1 9RS, United Kingdom or by e-mail to privacy@oviva.com. We will oblige their request except for any data which might be required for us to keep on file for a specified timeframe for compliance with applicable law(s), NHS standards/regulations, etc.

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 stores patient data for 8 years after the last interaction with the patient.
After this point the patient data is reviewed for whether it needs to be retained, and if not it is permanently erased from Oviva's electronic database. Oviva uses double deletion methods to erase data from its electronic database.

4.4

How will the data/information be archived?

Oviva will follow the guidance from NHS England and the Guidance on Appraisal produced by The National Archives.

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?

Oviva will fully follow NHS England and applicable data protection laws.

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. We only contact patients directly when it refers to an element of their care as part of their Oviva programme (such as Learn email content, automated enrolment emails etc) or a continuation of their care. When the comms are automated like this, the emails are sent via an API between OCS and SendGrid, database marketing.

If yes please detail.

Click here to enter text.

K) 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**
Data breach such as unauthorised access to systems or data.	Possible	Significant	Medium
Data leak such as data emailed to the wrong individual.	Possible	Significant	Medium
Data kept for longer than retention period.	Possible	Minimal	Low
Inaccurate data collected and processed.	Possible	Significant	Low
Possibility of sending PID to a GP practice (by Oviva) where the patient is no longer registered (e.g. due to changes in GP practice structures)	Possible	Minimal	Medium
Possibility that data subjects are not informed about the processing.	Possible	Minimal	Medium
Possibility that the Data controllers and processors do not have sufficient IG controls in place to provide assurance that they will handle personal data safely and securely	Possible	Significant	Medium
Data processed for a purpose unrelated to and incompatible with why it was collected.	Possible	Minimal	Low
More data collected than is necessary to meet defined purpose	Possible	Minimal	Low
Inadequate privacy information provided to data subjects	Possible	Minimal	Low

Issue with data transfer between GP practices and Oviva.	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)
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 (Secure Shell) 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 (time-based one-time password), password and smartkey, or TOTP, password and keyfiles	Reduced	Medium	
Data leak such as data emailed to the wrong individual.	Automatic email procedures to reduce human error. Staff training and awareness.	Reduced	Medium	
Data kept for longer than retention period.	Approve retention schedule, following NHS Records Management Code of	Tolerated	Low	

	Practice Process in place to delete records according to this schedule.			
Inaccurate data collected and processed.	Data directly provided by GP or patient. Verification process in place when processing GP referrals. Process to check certain data with patients. Patients are able to update and rectify data with the Patient Support Team where needed. Staff training and awareness.	Tolerated	Low	
Possibility of sending PID to a GP practice (by Oviva) where the patient is no longer registered (e.g. due to changes in GP practice structures)	Oviva to ask patients for an up to date GP practice when Oviva plans to send a communication to the GP practice	Reduced	Low	
Possibility that data subjects are not informed about the processing.	There is a clause in the Data Sharing Agreement (DSA) that obliged each Controller to ensure that its Privacy Notice is up to date and the nature of the sharing is actively communicated to patients. Therefore, all the controllers are responsible for updating their Privacy Notices to incorporate this processing. Oviva standard privacy to be included at the point where patients are referred to Oviva, which is made available at all times to Oviva's patients.	Reduced	Low	
Possibility that the Data controllers and processors do not have sufficient IG controls in place to provide assurance that they will handle personal data safely and securely	IG controls to be reviewed and monitored regularly at Oviva to ensure the sufficient controls in place. At Oviva we use two-factor authentication, strict password protocols, configuration management, and security monitoring and alerting software.	Reduced	Low	
Data processed for a purpose unrelated to	Data minimised to what is necessary, staff training and awareness, appropriate	Reduced	Low	

and incompatible with why it was collected.	policy and documents in place.			
More data collected than is necessary to meet defined purpose	Systems in place with specific sections for data capture so additional information cannot be added. GP and self-referral forms only capture data needed for a defined purpose. Staff training and awareness.	Reduced	Low	
Inadequate privacy information provided to data subjects	Privacy policy available online and linked in all letter and email communication with patients. DPO contact details available for all patients. Staff training and awareness.	Reduced	Low	
Issue with data transfer between GP Practices and Oviva.	Secure channel is utilised (via NHSmail) Password policy, staff training and awareness, access control, secure hosting and data minimised to what is necessary.	Reduced	Low	

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?
N/A

L) 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.
Click here to enter text.

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.

M) 7. DATA PROTECTION OFFICER COMMENTS AND OBSERVATIONS

7.1 **Comments/observations/specific issues**	Practices should review and update their privacy notice. Example text is provided below. Practices that use the SCW privacy notice

templates should add this to Appendix A.

Activity	Rationale
NHS Type 2 Transmission to Diabetes Remission Programme	**Purpose –** The NHS Type 2 Diabetes Path to Remission is a service for people with type 2 diabetes. It is a one-year programme to support healthier lifestyle, weight loss and remission of Type 2 diabetes. The programme consists of nutritionally complete total diet replacement products, for 12 weeks, followed by a period of food reintroduction and subsequent weight maintenance support, with a total duration of 12 months. The programme is delivered by Oviva, for any eligible patients referred by GPs in the eligible areas. The contract for the provision of the programme is held between NHSE and Oviva, with data flowing between Oviva and GP surgeries directly and between Oviva and the commissioners for reporting. Data is also provided to Buckinghamshire, Oxfordshire & Berkshire West ICB (only in aggregate form) to enable monitoring of referrals and ensure the overall success of the programme. **Legal Basis** – Direct Care under UK GDPR : • Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and • Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine

N) 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: 18/07/2023

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.

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.