Oxfordshire
Clinical Commissioning Group

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 :	13/10/2022
Title of the activity/processing:	Blood Collection Service
Who is the person leading this work?	[redacted]
Who is the Lead Organisation?	BOB ICB / CitySprint Couriers Ltd.
Who has prepared this DPIA?	[redacted]
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).	In Investment and Evolution (2019), GPC England and NHS England agreed to bring together current extended access services and funding streams under one, single funding stream under the Network Contract DES, to support delivery of a new model of 'Enhanced Access'. From 1 October 2022 Primary Care Networks (PCNs) will be required to provide Enhanced Access between the hours of 6.30pm and 8pm Mondays to Fridays and between 9am and 5pm on Saturdays (referred to as 'Network Standard Hours'). The new arrangements aim to remove variability across the country by putting in place a more standardised and better understood offer for patients. They will bring the Additional Roles Reimbursement Scheme (ARRS) workforce more consistently into the offer and support Primary Care Networks (PCNs) to use the Enhanced Access capacity for delivering routine services. The requirements are based on PCNs: • providing bookable appointments outside core hours within the Enhanced Access period of 6.30pm-8pm weekday evenings and 9am-5pm on Saturdays • utilising the full multi-disciplinary team • offering a range of general practice services, including 'routine' services such as screening, vaccinations and health checks, in line with patient preference and need, with PCNs having control over how the Enhanced Access capacity is used to manage the demand on practices To enable a range of GMS Services to be delivered during Network Standard Hours and support the requirements relating to a blended offer there was the need for Buckinghamshire, Oxfordshire and Berkshire West Integrated Care Board (BOB ICB) to commission a secure blood transportation service which would operate on Saturdays.

	The implementation of an efficient and secure blood transportation service, which is based on regular collections from pre-agreed collection point locations at pre-agreed times, will support PCNs' provision of Enhanced Access and enable a range of GMS Services to be effectively delivered. As its core, a Saturday blood transportation service will be delivered by the supplier, with blood samples collected from Oxfordshire GP Surgeries and taken to specimen laboratories. The collection routes will be determined by the information provided by PCNs in terms of their clinic locations and opening hours. In terms of sharing information patient data will be visible to the supplier due to the partly transparent nature of the specimen bags that the samples are sealed in. The recording / retention of patient data is not required by the service commissioned.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is)**.**	Oxfordshire PCNs / GP Practices, OUH & RBH Pathology, CitySprint Courier Services Ltd (Supplier)
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	No
Detail anything similar that has been undertaken before?	A weekday blood transportation service, managed by OUH, is currently in place, with a corresponding contract held with SCAS as the provider. Following confirmation that SCAS were unable to extend their service to include Saturdays, CitySprint Courier Services Ltd were put forward by the OUH as an alternative supplier and one who could meet the ICB's requirements.

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).	**Tick or leave blank** ✓

What statutory power or duty does the Controller derive their official authority from?
Data Protection Act 2018

Primary care commissioning and support duties under the NHS Act 2006 (Health and Social Care Act 2012) esp. Section 14S NHS Act 2006 duty to secure continuous improvement in the quality of primary medical services.

Processing is necessary for the performance of a task that is being carried out in the public interest as set out in the Background Information section of this DPIA and is proportionate to that purpose.

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?

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	**Tick or leave blank** ☐

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).	
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
Oxfordshire PCNs / GP Practices	Sole Controller
CitySprint Courier Services Ltd.	Processor

1.5.

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

The implementation of an efficient and secure blood transportation service, which is based on regular collections from pre-agreed collection point locations at pre-agreed times, will support PCNs' provision of Enhanced Access and enable a range of GMS Services to be effectively delivered.

A Saturday blood transportation service will be delivered by the supplier, with blood samples collected from Oxfordshire GP Surgeries and taken to designated specimen laboratories. The labels attached to individual specimen bottles detail Personal Data and Special Categories of Personal Data (name, address, NHS number,

tests required), which due to the partly transparent nature of the bags that the blood samples are sealed in, may be visible to the CitySprint couriers whose role is to solely collect and transport the specimens. The recording / retention of patient data is not required by the service commissioned.

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)

Personal Data / Special Category of Personal Data

1.7.

How are you satisfying the common law duty of confidentiality?

Reasonable expectations (please specify)

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

Processing the data is necessary for direct care purposes and is proportionate to that purpose. It is not possible to achieve the purpose without processing the data in the manner listed.

1.8.

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

No

If you are then describe what you are doing.

N/A

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.

1.10.

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

Unknown - non-specific patient cohort

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.)

Other method not listed

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

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

Visually

1.12.

How will you edit the data?

The data will not be edited.

1.13.

How will you quality check the data?

GP Practices: Personal Data / Special Category of Personal Data is detailed on the labels attached to individual specimen bottles, with the corresponding GP practice therefore responsible for the accuracy of this data.

The service that is being commissioned does not require the data to be quality checked, noting that it is not relevant to the service.

1.14.

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

Yes

If yes include in the risk section of this template.

1.15.

What training is planned to support this activity?

GP Practices: no training is required to support the service, with a weekday blood transportation service in place / operational, together with understanding in terms of responsibilities / inherent processes.

CitySprint Courier Services Ltd. (Supplier)

Upon employment staff are required to sign a confidentiality agreement and to complete Handling Medical Records, Personal and Sensitive Data an Introduction to Information Governance (IG) Training. Staff are required to re sit / undergo data protection training every 12 months, with daily reports listing the couriers whose training is in date and those near training expiry, ensuring training requirements are effectively met.

In addition:

- The Supplier shall ensure that all vehicle crew employed have undergone the appropriate training and awareness (or are trained and qualified) in the transportation and Carriage of Dangerous Goods (ADR 2019).
- The Supplier shall all ensure that any initial Good Distribution Practice (GDP) training completed by personnel shall be periodically supplemented with refresher training. This is to ensure personnel are up to date with all current ADR 2019 and Health & Safety legislative requirements.
- The Supplier also must be able to provide the appropriate evidence of training e.g. trained in refrigerant packaging or dry ice.
- The Supplier shall ensure that all vehicle crew employed have undergone the appropriate training and awareness (to trained and qualified) in the transportation of Controlled and precursor drugs.

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

2.1.

Are you proposing to combine any data sets?

No

If yes then provide the details here.

Click here to enter text.

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

Blood samples are collected from Oxfordshire GP Surgeries by CitySprint couriers and transferred securely to specimen laboratories. The collection routes will be determined by the information provided by PCNs in terms of their clinic locations and opening hours.

Inherent to the process, individual specimen bottles are labelled with patients' Personal Data and Special Categories of Personal Data (name, address, NHS number, tests required), and sealed in partly transparent bags. Upon arrival, in order to ensure minimised exposure of data, the bags are to be placed by practice staff into the opaque 'blood boxes', provided by the couriers, which are then to be transported to the designated pathology labs, with the bags subsequently removed from the 'blood boxes' by staff working within the labs.

CitySprint Courier Services Ltd. (Supplier)
The supplier shall ensure their vehicles or vehicles used in the delivery and performance the service comply with the relevant transport regulations. The supplier shall provide full updates on deliveries with real-time GPS tracking and electronic proof of delivery for full chain of custody.

The Supplier shall ensure that they can provide roadworthy vehicles to provide the security and safety requirements using its own resources or those of a partner organisation(s), with requirements including, but not limited to:

- Vehicles with Global Positioning System (GPS)
- Temperature controlled vehicles
- Vehicles fitted with anti-theft devices
- Compliance with all vehicle requirements as Carriage of Controlled Drugs

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

- Name
- Address
- NHS Number
- Tests Required

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.

<u>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.</u>

2.5.
Who are you planning to share the data/information with?
CitySprint Courier Services Ltd. (Supplier)

2.6.
Why is this data/information being shared?

Blood samples are being collected for the purpose of the delivery of primary care services to patients. Due to the nature of the partly transparent bags that the specimens are sealed in data / information is shared visually with the supplier. It is not possible to achieve the purpose outlined without sharing the data in the manner listed.

2.7.
How will you share it? (Consider and detail all means of sharing)
The data is shared directly, with the information accessed visually by the supplier (see 2.2 Data Flows).

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?
In addition to the Data Processing Protocol, inherent to the NHS Standard Contract, individual Data Processing Agreements will also be held with Oxfordshire PCNs / Practices, noting their role as Data Controllers.

2.9.
What reports will be generated from this data/information?
As part of the contract management process the commissioner will be provided with weekly activity reports detailing the number of collections / deliveries / failed collections etc. No patient data will be used in the generation of such reports.

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.

CitySprint Courier Services Ltd, Ground Floor, Red Central, 60 High Street, Redhill, Surrey, RH1 1SH
Click here to enter text.
Click here to enter text.
Click here to enter text.
Click here to enter text.
Click here to enter text.

3.2

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

Name of organisation	Registered	Registration details or comments if not registered
CitySprint Courier Services Ltd	Yes	ZA090879
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

3.3

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

Name of organisation	Brief description of assurances obtained
CitySprint Courier Services Ltd	• The Supplier shall ensure that they are compliant with and operate to the ISO 27001 Information Security Management standards or equivalents including, but not limited to, Sarbanes-Oxley (SOX) controls, as set out in Framework Schedule 10 (ISO 27001 or equivalent) • The supplier shall ensure that they are compliant with quality management standards including ISO9001, ISO14001 • The Supplier shall ensure that they are compliant with Cyber Essentials as set out in Framework Schedule 9 (Cyber Essentials Scheme) • The Supplier shall ensure that data is secured in a manner that complies with the Government Security Classification Policy rating appropriate to the classification of the information and data. The Supplier shall ensure that the Government Security Classification Policy rating is also applied when information and data is transmitted across all applicable networks and/ or in line with the Buyers' requirements • General Data Protection Regulation (Comply)

Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

3.4

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
CitySprint Courier Services Ltd	8HT62	Not Published	
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

3.5

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

The commissioned service does not require the storage of data

3.6

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

The data is shared directly, with the information accessed visually by the supplier (see 2.2 Data Flows).

In line with the clauses detailed in the Data Protection Protocol, which is inherent to the NHS Standard Contact, suppliers are required to evidence / ensure:

- Personnel do not process Personal Data except in accordance with the Contract
- The implementation of technical and organizational measures to ensure the security of the data
- The reliability and integrity of any Personnel who have access to the Personal Data and ensure that they:
  - (A) are aware of and comply with the supplier's duties under the Data Protection Protocol
  - (B) are subject to appropriate confidentiality undertakings

(C)	are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party; and
(D)	have undergone adequate training in the use, care, protection and handling of Personal Data, which is completed every 12 months

3.7
Is there any use of Cloud technology?
No

If yes add the details here.
Click here to enter text.

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

Upon employment CitySprint Courier Services Ltd. staff are required to sign a confidentiality agreement and to complete Handling Medical Records, Personal and Sensitive Data an Introduction to Information Governance (IG) Training. Staff are required to re sit / undergo data protection training every 12 months, with daily reports listing the couriers whose training is in date and those near training expiry, ensuring training requirements are effectively met. In addition, ensuring training compliance, once a courier's training has expired it is not possible for the Supplier's Operations Controllers to allocate ' bookings' to the courier until the corresponding training has been completed.

The Supplier is required to ensure that the staff involved in the performance of the contract:

(a) be DBS checked
(b) be appropriately trained and qualified
(c) be vetted using Good Industry Practice and the Security Policy
(d) comply with all conduct requirements when on the Buyer's Premises
(e) carry relevant photographic identification upon their person at all times including but not limited to:
  - A UK driving licence
  - Photo identity cards
  - Organisation identity cards

The supplier is required to ensure their vehicles or vehicles used in the delivery and performance the service comply with the relevant transport regulations. The supplier shall provide full updates on deliveries with real-time GPS tracking and electronic proof of delivery for full chain of custody.

The supplier shall ensure that they can provide roadworthy vehicles to provide the security and safety requirements using its own resources or those of a partner organisation(s), with requirements including, but not limited to:

- Vehicles with Global Positioning System (GPS)
- Temperature controlled vehicles
- Vehicles fitted with anti-theft devices
- Compliance with all vehicle requirements as Carriage of Controlled Drugs

Is a specific System Level Security Policy needed?
No

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

3.9

Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

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

Click here to enter text.

3.10

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

A Data Processing Protocol is inherent to the NHS Standard Contract, with BOB ICB responsible for its management. Individual Data Processing Agreements will also be held with Oxfordshire PCNs / Practices, noting their role as Data Controllers.

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).

Privacy Notice displayed in practices and practice websites to be updated with inclusion of CitySprint on the list of data processors

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).

N/A

4.3

How long is the data/information to be retained?

The commissioned service does not require the retention of data

4.4

How will the data/information be archived?

The commissioned service does not require the archiving of data

4.5

What is the process for the destruction of records?

N/A

4.6

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

All access to data will cease, with no data recorded, retained or archived

4.7

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

No

If yes please detail.

Click here to enter text.

5. Risks and Issues

5.1

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

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Patient information may be shared without their knowledge	Possible	Significant	Medium
Risk of data loss due to the transportation of labelled specimens	Possible	Significant	High
Highly sensitive data will be accessed by a third party	Probable	Significant	Medium
Risk of non-compliance with the GDPR due to inadequate contractual arrangements	Possible	Significant	High
Access to personal data is unauthorised	Possible	Significant	High

5.2

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

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Patient information may be shared without their knowledge	Ensure Privacy Notices are updated to include CitySprint on the list of data processors	Reduced	Low	Choose an item.
Risk of data loss due to transportation of labelled specimens	Ensure supplier's transport logistics enable safe and secure movement of specimens, with robust SOP in place	Reduced	Medium	Choose an item.
Highly sensitive data will be accessed by a third party	Review of supplier's security / training accreditations	Reduced	Low	Choose an item.
Risk of non-compliance with the GDPR due to inadequate contractual arrangements	Data Processing Protocol / Agreement(s) to be in place, with the nature of the processing detailed alongside the contract	Reduced	Low	Choose an item.

Access to personal data is unauthorised	Ensure supplier has appropriate security measures / accreditation in place	Reduced	Medium	

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

6. Consultation

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

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
CitySprint Courier Services Ltd, with input provided in terms of completion

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	

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 (BOB ICB)

Name: [redacted]

Job Title: Data Protection Officer

Signature: [redacted] Date: 17/10/2022

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.