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 :	21/07/2022
Title of the activity/processing:	Local Risk Management System - Blueteq
Who is the person leading this work?	[redacted]
Who is the Lead Organisation?	BOB ICB
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).	Streamline processes established in the 3 x places to form a single Local Risk Management System with Blueteq Other systems used currently are a mix of Datix instances and spreadsheets.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	No – the 3 x former CCGs are now a single entity – BOB ICB
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?	Each place already has a similar LRMS or multiple systems achieving the same purpose. The platform is already used across BOB for Prior Approvals. The processes and data flows are the same as currently used in places with different systems.

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?
For PALS/Complaint services the person is giving direct consent to sharing their information in order to resolve concerns regarding their healthcare and access to services.

What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom).
Verbal or written via engagement with the PALS/Complaints team

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?
The system is used to manage complaints, patient safety incidents, record safeguarding advice which can be shared in a meaningful manner and to allow a method of triangulating source of information.
The ICB is required to perform these functions under NHS act 2006 as amended, and the Health and Social Care act 2022.

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?

The system is used to manage complaints, patient safety incidents, record safeguarding advice which can be shared in a meaningful manner and to allow a method of triangulating source of information.

Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	**Tick or leave blank** ✓
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	**Tick or leave blank** ☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*
e) The data has been made public by the data subject	*NA*
f) For legal claims or courts operating in their judicial category	*NA*
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE OR OCCUPATIONAL MEDICINE, FOR THE ASSESSMENT OF THE WORKING CAPACITY OF THE EMPLOYEE, MEDICAL DIAGNOSIS, THE PROVISION OF HEALTH OR SOCIAL CARE OR TREATMENT OR THE MANAGEMENT OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ✓
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☑
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT.	**Tick or leave blank** ☐

(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	

1.3.

If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to i). NOTE: d), e) and f) are not applicable

1.4.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board	Sole Controller
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
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?

PALS/Complaints will receive contacts from patients/carers/relatives/public to express concerns and receive advice on how to manage them. These may relate to individual circumstances which are described and recorded. The safeguarding team will record information relating to protection of individuals and the advice given to clinicians responsible for their care. Legal basis: Consent, Condition for processing: 9 2 (a) consent
The patient safety team will record incidents declared by providers relating to patient safety and quality, in the scope of national guidance – and the action taken to mitigate risks to patient safety. Legal basis: 6 1 (e) Public Task, Condition for processing: 9 2 (h) or 9 2 (i)
Healthcare professional from external providers may input feedback which may will consist of a log of clinical concerns and may record an NHS number as well as a narrative description to share with healthcare professionals who can review potential risks to quality and safety. Legal basis: 6 1 (e) Public Task, Condition for processing: 9 2 (h) or 9 2 (i)

The processing is in line with a mixture of legal obligations (safeguarding) and NHS requirements and guidance.

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)
The information included will include reference to clinical records

1.7.
How are you satisfying the common law duty of confidentiality?
Legal Duty (please specify)

Consent (Explicit or implied)

If you have selected an option which asks for further information please enter it here
Legal Duty – safeguarding, pseudonymized/anonymized patient safety incidents and healthcare professional feedback, substantial public interest in addressing concerns with the quality and safety of healthcare services, implied consent and informed consent for PALS.

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.
Use of NHS Number only to share information with external providers to investigate and for healthcare professional feedback to an individual case.

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.
Described above – for management of patient safety and quality of healthcare

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.)
Electronic form
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.
PALS & Complaints may receive phone/email/letter from patient and enter case onto Blueteq. HCPs may in future log an incident via front-end form and be able to view their own submitted form but no further data. Access to the Platform by authorised users at the ICB and Providers granted with security groups and restricted, password access

1.12.
How will you edit the data?
Via platform with security groups and restricted, password access

1.13.
How will you quality check the data?

Data entry responsible for quality of information submitted. No checking of nhs# against the Spine is carried out to verify.

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?
Training of users, along with general training of those external reporters

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).
Internal reporters within the ICB (eg PALS and Complaints) recording directly to platform, some external reporters recording to web form, before data passed to those in other organisations via secured link, or password access. Reports can be created by authorised users only, aggregated data only can be shared. Personal data (nhs#) is shared only with investigator(s) for that incident.

2.3.
What data/information are you planning to share?
For internal systems (e.g PALS/complaints) none, for external (e.g. patient safety) description of patient safety issue and NHS number to allow for appropriate identification and investigation.

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?
Professionals directly responsible for quality and patient safety within healthcare providers

2.6.
Why is this data/information being shared?
To review concerns and risks to quality and patient safety, and to investigate complaints.

2.7.
How will you share it? (Consider and detail all means of sharing)
Via secure platform (Blueteq)

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
Security and password access – only relevant information is collected and stored for any individual system

2.8.
What data sharing agreements are or will be in place?
No specific sharing agreements are required.

2.9.
What reports will be generated from this data/information?
Aggregated data for high-level reports for relevant ICB committees.

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.
Blueteq Ltd
Unit 5, Endeavour Business Park, Penner Road, Havant, PO9 1QN
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
Blueteq	Yes	Z2946230
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
Blueteq Ltd	DSP Toolkit compliant with audit results for past 5 years
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
Blueteq Ltd	8HR52	Standards Met	28/03/2022
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).

Secure servers based in England, owned by Blueteq

3.6

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

Password and RBAC security group protection grants permissions. Users are only authorised to access cases relevant to the purpose.

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?
Encryption at rest and in transit. Access via RBAC login controlled by ICB. Blueteq do not have access to any data within the system.

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?
Services Contract is in place with Blueteq with ID and Data Processing clauses, ICB is Controller

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).
Purpose of processing is already in the ICB Privacy Notice. Blueteq as system supplier is not required to be listed separately.

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).
No change to individual rights, requests will be managed under existing policy.

4.3
How long is the data/information to be retained?
Data remains under control of ICB, retained in accordance with NHSE Code of Practice on Records Management and BOB ICB RM Policy and retention schedule. Records are kept for 30 years if SIRI, other records will be 10 years.

4.4
How will the data/information be archived?
In accordance with policy (see above) no data is archived. Information is current within the database, or deleted when expired.

4.5
What is the process for the destruction of records?
Electronic deletion.

4.6
What will happen to the data/information if any part of your activity ends?
Data will be extracted by Blueteq and transferred back to ICB on end of contract (relevant clause included in contract). Activity by ICB and purpose for processing is legal requirement.

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**
Unauthorised access to personal data or unauthorised disclosure	Possible	Significant	Medium
Loss of data by system malfunction or misconfiguration, or during transfer to Blueteq from existing system	Possible	Significant	Medium
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.

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)**
Unauthorised access to personal data or unauthorised disclosure	RBAC controls to database managed by IBC, NHS# to be shared with nominated lead at investigating org to identify patient when relevant; all staff complete annual IG training and are aware of responsibilities to protect data	Reduced	Low	Choose an item.
Loss of data by system malfunction or misconfiguration, or during transfer to Blueteq from existing system	ICB is responsible for configuration of database by trained staff; review of requirements and solution with testing is carried out appropriately before system changes; amount of personal data held within system is minimised. Extraction of	Reduced	Low	Choose an item.

	data prior to transfer to Blueteq will be done by ICB staff, means of transfer is by .csv file via nhs.net to nhs.net			
There is a risk to business continuity by either an issue preventing Blueteq from hosting an effective system, or by hardware or software issues affected BOB ICB	Blueteq are responsible for the maintenance and development of the Blueteq system and servers. BOB ICB is supported by SCWCSU for IM&T – there is a risk this will affect BOB ICB teams being able to use systems they rely upon and rely on use of spreadsheets to temporarily manage new and emergent cases – the shared email mailboxes will contain correspondence to support ongoing dialogue with regard to cases.	Tolerated	Low	Choose an item.
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?
End of contract with Blueteq

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
Click here to enter text.

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.

7. Data Protection Officer Comments and Observations

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

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 South, Central and West CSU

Name: [redacted]

Job Title: Strategic IG Lead

Signature: [redacted] Date: 29/07/2022

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: 01/08/2022

Please note:

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

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here:
Click here to enter text.