

## 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 <b>MUST</b> carry out a DPIA where you plan to:	Tick or leave blank
Use <b>profiling or automated decision-making</b> to make significant decisions about people or their access to a service, opportunity or benefit;	<input type="checkbox"/>
Process <b>special-category data or criminal-offence data on a large scale</b> ;	<input type="checkbox"/>
<b>Monitor a publicly accessible place</b> on a large scale;	<input type="checkbox"/>
Use <b>innovative technology</b> in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Carry out <b>profiling</b> on a large scale;	<input type="checkbox"/>
<b>Process biometric or genetic data</b> in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
<b>Combine, compare or match data</b> from multiple sources;	<input type="checkbox"/>
Process personal data <b>without providing a privacy notice</b> directly to the individual in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
	<input type="checkbox"/>
Process <b>children's</b> personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	<input type="checkbox"/>
Process personal data that could result in a <b>risk of physical harm</b> in the event of a security breach.	<input type="checkbox"/>

You as Controller should <b>consider</b> carrying out a DPIA where you	Tick or leave blank
Plan any major project involving the use of personal data;	<input type="checkbox"/>
Plan to do evaluation or scoring;	<input type="checkbox"/>
Want to use systematic monitoring;	<input type="checkbox"/>
Process sensitive data or data of a highly personal nature;	<input type="checkbox"/>
Processing data on a large scale;	<input type="checkbox"/>
Include data concerning vulnerable data subjects;	<input type="checkbox"/>
Plan to use innovative technological or organisational solutions;	<input checked="" type="checkbox"/>

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	
<b>Date of your DPIA :</b>	28/08/2023
<b>Title of the activity/processing:</b>	BOB ICB Primary Care Strategy – Analytics
<b>Who is the person leading this work?</b>	██████████
<b>Who is the Lead Organisation?</b>	BOB ICB
<b>Who has prepared this DPIA?</b>	██████████
<b>Who is your Data Protection Officer (DPO)?</b>	██████████
<b>Describe what you are proposing to do:</b> (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	BOB ICB has asked KPMG to support the development of a Primary Care Strategy. KPMG wish to analyse healthcare system utilisation across time, geography, type of service, provider, patient demographics, and other variables. Data to be provided by SCW at aggregate level, which KPMG will use alongside public domain data sets to inform BOB ICB primary care strategy.
<b>Are there multiple organisations involved?</b> (If yes – you can use this space to name them, and who their key contact for this work is).	No
<b>Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA?</b> (If so then include the details here).	SCW KPMG
<b>Detail anything similar that has been undertaken before?</b>	KPMG is doing a similar project with Northwest London ICB.

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use		
<b>1.</b>		
<b>What data/information will be used?</b> Tick all that apply.	Tick or leave blank	<b>Complete</b>
Personal Data	<input type="checkbox"/>	1.2
Special Categories of Personal Data	<input type="checkbox"/>	1.2 AND 1.3
Personal Confidential Data	<input type="checkbox"/>	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data )	<input type="checkbox"/>	1.2 but speak to your IG advisor first
Pseudonymised Data	<input type="checkbox"/>	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	<input checked="" type="checkbox"/>	Consider at what point the data is to be anonymised
Commercially Confidential Information	<input type="checkbox"/>	Consider if a DPIA is appropriate
Other	<input type="checkbox"/>	Consider if a DPIA is appropriate
<b>1.1.</b>		
<b>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.</b>		
Article 6 (1) of the GDPR includes the following:		
a) THE DATA SUBJECT HAS GIVEN CONSENT	<input type="checkbox"/>	Tick or leave blank
b)	<input type="checkbox"/>	

<b>Why are you relying on consent from the data subject?</b> Click here to enter text.	
<b>What is the process for obtaining and recording consent from the Data Subject?</b> (How, where, when, by whom). Click here to enter text.	
<b>Describe how your consent form is compliant with the Data Protection requirements?</b> (There is a checklist that can be used to assess this). Click here to enter text.	
<b>c) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY</b>  (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).	<b>Tick or leave blank</b> <input type="checkbox"/>
<b>What contract is being referred to?</b> Click here to enter text.	
<b>d) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT</b>  (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).	<b>Tick or leave blank</b> <input type="checkbox"/>
<b>Identify the legislation or legal obligation you believe requires you to undertake this processing.</b> Click here to enter text.	
<b>e) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON</b>  (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).	<b>Tick or leave blank</b> <input type="checkbox"/>
<b>How will you protect the vital interests of the data subject or another natural person by undertaking this activity?</b> Click here to enter text.	
<b>f) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER</b>  (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).	<b>Tick or leave blank</b> <input checked="" type="checkbox"/>
<b>What statutory power or duty does the Controller derive their official authority from?</b> National Health Service Act 2006, as amended by the Health and Social Care Act 2012 and the Health and Care Act - Duty as to improvement in quality of services.	
<b>g) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY</b>  (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).	<b>Tick or leave blank</b> <input type="checkbox"/>
<b>What are the legitimate interests you have?</b> To look at improving the health and wellbeing of the local population. Data is all anonymised so only aggregate data used to develop strategy.	
Article 9 (2) conditions are as follows:	
<b>a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT</b>  (Requirements for consent are the same as those detailed above in section 1.2, a))	<b>Tick or leave blank</b> <input type="checkbox"/>

<b>b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION</b> (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 <input type="checkbox"/>
<b>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</b> (Requirements for this are the same as those detailed above in section 1.2, d))	Tick or leave blank <input type="checkbox"/>
<i>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</i>	NA
<i>e) The data has been made public by the data subject</i>	NA
<i>f) For legal claims or courts operating in their judicial category</i>	NA
<b>g) SUBSTANTIAL PUBLIC INTEREST</b> (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 <input type="checkbox"/>
<b>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</b> (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 <input checked="" type="checkbox"/>
<b>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</b> (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 <input type="checkbox"/>
<b>j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH <u>ARTICLE 89(1)</u> 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.</b> (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 <input type="checkbox"/>

### 1.2.

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  
**N/A**

### 1.3.

**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
BOB ICB	Sole Controller

KPMG	Processor
SCW CSU	Processor
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.

**1.4.**

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

For patients where BOB ICB is the commissioner: Emergency Care Dataset (A&E), GP attendance data (from EMIS), NHS 111 data, community data and 999 data is being processed by SCW CSU. SCW CSU are extracting the data from EPRs/data warehouses and aggregating it with small number suppression rules applied. KPMG is then analysing the data to understand historical demand and predict future demand for these services to help inform the ICB's primary care strategy.

**1.5.**

**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)

**1.6.**

**How are you satisfying the common law duty of confidentiality?**

No disclosure due to anon/pseudo actions

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

Click here to enter text.

**1.7.**

**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.**

SCW CSU is aggregating the data and applying small number suppression rules

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

**1.8.**

**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.**

Purpose is to understand historical demand and predict future demand for services to help inform the ICB's primary care strategy

<p><b>1.9.</b> <b>Approximately how many people will be the subject of the processing?</b> STP population</p>
<p><b>1.10.</b> <b>How are you collecting the data?</b> (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. Choose an item.</p> <p><b>If you have selected 'other method not listed' describe what that method is.</b></p> <p>Using aggregated data from electronic patient records, and publicly available data sets (NHSE, ONS)</p>
<p><b>1.11.</b> <b>How will you edit the data?</b></p> <p>KPMG will not edit the data – it will be used for analysis in the state provided.</p>
<p><b>1.12.</b> <b>How will you quality check the data?</b></p> <p>KPMG will not quality check the supplied data but will compare counts against public data sets.</p>
<p><b>1.13.</b> <b>Review your business continuity or contingency plans to include this activity. Have you identified any risks?</b> Yes <b>If yes include in the risk section of this template.</b></p>
<p><b>1.14.</b> <b>What training is planned to support this activity?</b> N/A</p>
<p><b>2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital</b></p>
<p><b>2.1.</b> <b>Are you proposing to combine any data sets?</b> No <b>If yes then provide the details here.</b> KPMG will not be combining data at an individual level as all data provided will be aggregated and anonymised.</p>
<p><b>2.2.</b> <b>What are the Data Flows?</b> (Detail and/or attach a diagram if you have one).</p>

Data will flow from a number of different sources including Acute, Community Providers and Primary Care either extracted directly or processed via NHSE as a recognised local or national commissioning flow. SCW will aggregate and anonymise before sending securely to KPMG.

**2.3.**

**What data/information are you planning to share?**

KPMG will not share data - For patients where BOB ICB is the commissioner: Emergency Care Dataset (A&E), GP attendance data (from EMIS), NHS 111 data, community data and 999 data is being processed by SCW CSU. SCW CSU are extracting the data from EPRs/data warehouses and aggregating it with small number suppression rules applied. The data will then be shared with KPMG via secure file transfer.

**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**

N/A

**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?**

KPMG will analyze data and share results with BOB ICB only.

**2.6.**

**Why is this data/information being shared?**

Data (aggregated, anonymous) is being shared with KPMG so that they can analyse it as part of the Primary Care Strategy work they are doing for BOB ICB

**2.7.**

**How will you share it?** (Consider and detail all means of sharing)

Data will be shared with KPMG using KPMG's secure file transfer mechanism, LFT (Large File Transfer).

**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**

N/A

**3.**

**What data sharing agreements are or will be in place?**

There are no data sharing agreements in place as this work does not involve sharing personal data between data controllers.

**3.1.**

**What reports will be generated from this data/information?**

KPMG will analyse the data to understand historical demand and predict future demand for services to help inform the ICB's primary care strategy. KPMG will only share the output of their analysis with the ICB. This will be provided at summary level in PowerPoint slides for a workshop and in strategy documents.

**3.2.**

**Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?**

No

**If yes, are all the right agreements in place?**

**Give details of the agreement that you believe covers the use of the NHSD data**

N/A

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.**

KPMG LLP, 15 Canada Square, London, E14 5GL

SCW CSU , Omega House, Eastleigh, SO50 5PB

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
KPMG LLP	Yes	Z7047609 ( <a href="#">certificate available here</a> )
SCW	Yes	Z2950066
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
KPMG LLP	Registered with ICO. Contract in place with BOB. KPMG LLP is ISO 27001 certified (the international standard of information security



	management). KPMG LLP is also certified to the first level of Cyber Essentials (a UK government cyber security standard). KPMG provides all its staff with regular training on data protection and confidentiality. Annual training is mandatory for all staff and completion of training modules is monitored. KPMG’s training and awareness programs have been reviewed and updated as part of their GDPR Compliance Programme. All KPMG employees are required to sign an annual Ethics and Independence Confirmation. This confirmation includes a declaration of commitment to confidentiality, data privacy, transactions and affairs of clients and a declaration of commitment to information security. All KPMG employees with access to information resources are provided with a user and password ID that has been specifically assigned to them.
SCW CSU, Omega House, Eastleigh, SO50 5PB	ICO registered, Cyber Security Essentials+ Accredited and GDPR compliant. BOB ICB and SCW SLA
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
KPMG LLP	8J871	22/23 Standards Exceeded	20/06/2023
SCW	ODF	Standards exceeded	22/06/2023
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).

KPMG will store the aggregated anonymised data in a folder on their secure shared drive, which will only be accessible to analytics team staff members working on the engagement. Controlled using file system permissions. Storage is on KPMG’s own servers.

### 3.6

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

It will be accessed via the folder on the secure shared drive and will only be accessible to staff members working on the engagement. Files will be password-protected.

### 3.7

#### Is there any use of Cloud technology?

No

If yes add the details here.

N/A

**3.8**

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

KPMG LLP is ISO 27001 certified (the international standard of information security management). KPMG LLP is also certified to the first level of Cyber Essentials (a UK government cyber security standard). KPMG provides all its staff with regular training on data protection and confidentiality. Annual training is mandatory for all staff and completion of training modules is monitored. KPMG's training and awareness programs have been reviewed and updated as part of their GDPR Compliance Programme. All KPMG employees are required to sign an annual Ethics and Independence Confirmation. This confirmation includes a declaration of commitment to confidentiality, data privacy, transactions and affairs of clients and a declaration of commitment to information security. All KPMG employees with access to information resources are provided with a user and password ID that has been specifically assigned to them.

**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.**

N/A

**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?**

Only aggregated data will be sent to KPMG. BOB ICB has awarded a one-off contract to KPMG to carry out a specific analysis for the Primary Care Strategy. SCW CSU has an SLA in place to process personal data on behalf of BOB ICB.

**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).

None

**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).

Only aggregated data will be supplied to KPMG no impact on the individual rights.

**4.3**

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

3 years in line with KPMG's retention policy.

**4.4**

**How will the data/information be archived?**

Data will remain accessible to authorised personnel until destruction.

**4.5**

**What is the process for the destruction of records?**

Physical deletion from secure shared drive.

KPMG uses a leading third-party service provider for media destruction to pulverise ‘end of life’ electronic media devices. The supplier is certified to ISO 27001 and the NCSC CAS-S. ‘End of life’ KPMG PCs and hard drives are erased using recognised industry erasure software to HMG InfoSec Standard 5 compliant settings. All server disks that are ‘end of life’ are degaussed and destroyed through certified destruction via a reputable third-party supplier.

**4.6**

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

Physical deletion from secure shared drive. See 4.5 for drive destruction at End of Life.

**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. <small>(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)).</small>	Likelihood of harm	Severity of harm	Overall risk
Unauthorised access to KPMG folder	Remote	Minimal	Low
KPMG system hacked	Remote	Minimal	Low
<a href="#">Click here to enter text.</a>	<a href="#">Choose an item.</a>	<a href="#">Choose an item.</a>	<a href="#">Choose an item.</a>
<a href="#">Click here to enter text.</a>	<a href="#">Choose an item.</a>	<a href="#">Choose an item.</a>	<a href="#">Choose an item.</a>

**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 KPMG folder	KPMG access controls are in place. No personal data stored.	Tolerated	Low	No
KPMG system hacked	KPMG have appropriate security and technical	Tolerated	Low	No

	controls in place. No personal data stored.			
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.

### 5.3

#### What if anything would affect this piece of work?

None known.

### 5.4

#### Please include any additional comments that do not fit elsewhere in the DPIA?

None

## 6. Consultation

### 6.1

#### Have you consulted with any external organisation about this DPIA?

No

#### If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.

N/A

### 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.

N/A

## 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 SCW CSU

Name: [Redacted]

Job Title: Senior Information Governance Manager

Signature: [Redacted]

Date: 12/09/2023

Signed and approved on behalf of Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board

Name: [Redacted]

Job Title: Data Protection Officer

Signature: [Redacted]

Date: 13/09/2023

**Please note:**

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

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

Click here to enter text.