



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;	<input type="checkbox"/>
Process special-category data or criminal-offence data on a large scale ;	<input checked="" type="checkbox"/>
Monitor a publicly accessible place on a large scale;	<input type="checkbox"/>
Use innovative technology in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Carry out profiling on a large scale;	<input type="checkbox"/>
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Combine, compare or match data from multiple sources;	<input type="checkbox"/>
Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
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;	<input type="checkbox"/>
Process children's 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 risk of physical harm in the event of a security breach.	<input checked="" type="checkbox"/>

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;	<input checked="" 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 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	
Date of your DPIA :	01/07/2023
Title of the activity/processing:	Lloyd George Records Storage and Management Service
Who is the person leading this work?	██████████
Who is the Lead Organisation?	Buckinghamshire, Oxfordshire, and Berkshire West Integrated Care Board (BOB ICB)/ Offsite Archive Storage & Integrated Services (UK) Ltd (OASIS Group) – “OASIS”
Who has prepared this DPIA?	██████████
Who is your Data Protection Officer (DPO)?	██████████ ICB DPO ██████████ BOB GP DPO – comments section 7
<p>Describe what you are proposing to do:</p> <p>(Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).</p>	<p>BOB ICB are commissioning and off-site storage solution with a scan-on-demand (SCOD) function to incorporate 23 practices across Buckinghamshire, Berkshire West, and Oxfordshire.</p> <p>With a total list size of around 320,000 there is a requirement to collect and reconstitute patient records from Iron Mountain UK Ltd.’s premises and corresponding GP practices and to subsequently store the records and provide a SCOD service to the practices.</p> <p>Approximately 60% of the records are held at Iron Mountain’s warehouse locations with the remaining records held at the corresponding practices and in storage facilities.</p> <p>A large number of records that are held at Iron Mountain’s warehouses were removed from their envelopes when the records were being scanned by Iron Mountain. The records may be separated by a blank paper or held together with rubber bands. In such cases, there is the need for thorough organization and for each record to be placed in a suitable file/envelope.</p> <p>When reconstituting the records from Iron Mountain, there may be occasions where the individual patient records are identified and/or found to contain records of multiple patients. OASIS will mark these as exceptions and return them to the relevant practice for full reconstitution.</p> <p>When multiple patients in an individual record are <u>not identified and /or found</u> during the reconstitution process but are found at a later date (e.g. SCOD request) OASIS will mark these as exceptions and return them to the relevant practice for full reconstitution.</p> <p>Please refer to section 6A “Variation to standard specification” in the service Level Agreement (order form) for the relevant clause.</p>

The clause only applies to records that have been collected from Iron Mountain and not to records collected from the Practices.

The collection and reconstitution process of the records from their current locations is to be completed one practice at a time, the order of which will be determined by the ICB. Once a practice's records have been collected from the Iron Mountain's warehouse and the corresponding practice, they will be individually indexed using the NHS number and used for tracking and auditing purposes.

OASIS shall use their best endeavours to complete collation / indexing of records for all of the 17 practices (figure includes branch sites and at offsite storage locations) within **10 weeks** of contract signature.

In terms of indexing all records, including empty wallets/files are to be allocated a unique barcode reference ensuring that records can be always tracked which will enable practices to request the return of records / SCODs as and when required.

Upon completion of indexing, an inventory of the records is to be shared with the practices with a review completed to ensure:

- Data is captured for a full list of records, with reconciliation against practice lists.
- Any discrepancies are identified and rectified together with the practice and with Iron Mountain. Oasis will liaise with Iron Mountain with support from the ICB team if required.
- All relevant staff have been trained and are fully aware of processes relating to the return and collection of records etc.

A pilot trial will be completed prior to the commencement of the full transfer. During this trial, an agreed number of records will be transferred to OASIS's site, with both BOB ICB and OASIS project management teams in attendance.

During this, OASIS will collaborate with the ICB to review:

- The condition of the records as received from Iron Mountain
- How the records are packed prior to transportation
- How individual records are identified.
- How individual records will be separated and covered.

The results from this trial will be analysed, to develop adjustments to drive continuous improvement and enact remedial measures using practical evidence. All processes will be reviewed to ensure they are effective and efficient, with any corrective actions developed and implemented prior to commencement of the full project.

For each load of records received from Iron Mountain, the NHS Number will be captured upon receipt at OASIS's facility.

	<p>Data Capture / entry timescales is dependent on the size of the practice (see below):</p> <p>Timescales based on 5 indexers.</p> <p>> 5,000 list Practice - cataloguing complete 2 working days.</p> <p>>10,000 list Practice - cataloguing complete 4 working days.</p> <p>>15,000 list Practice - cataloguing complete 6 working days.</p> <p>>20,000 list Practice - cataloguing complete 8 working days.</p> <p>1 indexer = 500 to 750 Patient records per day (type in 10 digit NHS No / place barcode on patient record and scan to box.</p> <p>This will also be dependent on the additional piece of work / step to place records back into folders.</p> <p>Speculative - 60 seconds per additional step</p> <p>Pilot required to evaluate the extra step.</p> <p>The project team at OASIS will be responsible for the transfer and data entry of records currently held by the practices who were yet to have their notes collected by Iron Mountain. This project team will be responsible for attending each practice location, packing records according to pre-agreed criteria, and transportation to OASIS's facility. A specialist Date Entry team will enter the data each load of records will be completed as per the timescales specified above.</p> <p>Practices that have their records digitised by Iron Mountain and uploaded onto the Emis clinical system will have new patient records that are transferring into the Practice.</p> <p>These Practices will require their new patient paper records to be collected. A quarterly collection with delivery will be arranged with the practice and a Scan-on-demand service provided. Ad-Hoc requests may also be made by the Practices.</p> <p>The OASIS records management system allows for the development of a full audit trail, with all actions taken on an item (i.e., picked, ordered, delivered to practice), are tracked using their tracking solutions. All workflows used by OASIS have several key points at which the item's unique barcode will be scanned, with its location and other key details automatically uploaded to the records management system.</p> <p>Practice Teams will use the 'noteSpace' desktop application (secure portal) to securely request the return of paper Lloyd George records held in storage with OASIS, the collection of paper Lloyd George records from the Practice and Scan on Demands.</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Practices will control which staff are authorised to use the noteSpace application.</p> <p>Remote online training on how to use the noteSpace application will be provided to Practices and ongoing support provided by OASIS Client Care Team. Contact details for the Client Care Team will be provided and that Team will for example, be the point of contact for ordering boxes or box barcodes.</p> <p>Accreditations are to be in place, with required standards met in relation to the safe and secure handling of data. No data is to be transferred outside of the UK.</p> <p>For the full duration of this Project, effective engagement is required with both Iron Mountain and with each of the practices, with corresponding training and access to portals.</p>
<p>Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).</p>	Iron Mountain (current supplier) / GP Practices / OASIS Group (new supplier)
<p>Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).</p>	No
<p>Detail anything similar that has been undertaken before?</p>	BOB ICB and a number of GP practices currently hold direct contracts with suppliers (including OASIS) who provide an off-site storage / record management service. This process involves the boxing up, removal, and storage of paper records including a SCOD service whereby the practice can request digital records on an ad hoc basis.

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	<input checked="" type="checkbox"/>	1.2
Special Categories of Personal Data	<input checked="" type="checkbox"/>	1.2 AND 1.3
Personal Confidential Data	<input checked="" type="checkbox"/>	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data)	<input checked="" 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

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 <input type="checkbox"/>
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	Tick or leave blank <input type="checkbox"/>
(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).	
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	Tick or leave blank <input type="checkbox"/>
(A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	
Identify the legislation or legal obligation you believe requires you to undertake this processing. Click here to enter text.	
d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON	Tick or leave blank <input type="checkbox"/>
(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).	
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	Tick or leave blank <input checked="" type="checkbox"/>
(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).	
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 of data held within the Lloyd George Record is essential for the performance of a task that is being carried out in the public interest. The public interest benefits include: <ul style="list-style-type: none"> • Reduced need for additional space in some GP practices/ PCN networks or for building extensions or practice relocation. • Additional capacity for collaboration across primary care networks. 	

The above public interests cannot be achieved without processing the data as set out in the Background Information section of this DPIA. Processing the data is necessary to enable the realisation of the public benefits listed above and is proportionate to that purpose. It is not possible to realise these benefits without processing the data in the manner listed.	
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 <input type="checkbox"/>
What are the legitimate interests you have? Click here to enter text.	
Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	Tick or leave blank <input type="checkbox"/>
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 <input type="checkbox"/>
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 <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
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 <input type="checkbox"/>
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 <input checked="" type="checkbox"/>
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 <input type="checkbox"/>

<p>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.</p> <p>(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).</p>	<p>Tick or leave blank</p> <p><input type="checkbox"/></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------

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).

Records held at both Iron Mountain and Practice premises	
Name of Organisation	Role
Burma Hill Surgery	Sole Controller
Balmore Park Surgery	Sole Controller
Unity Health (Chinnor, P. Risborough, Thame Health [Brill Surgery, Thame Health Centre, Crendon Surgery])	Sole Controller
<i>Leave blank</i>	<i>Other</i>
Records held at Practice premises only	
Name of Organisation	Role
*Millbarn Medical Centre	Sole Controller
London Street Surgery	Sole Controller
Whitehill Surgery	Sole Controller
Emmer Green Surgery	Sole Controller
The John Hampden Surgery	Sole Controller
**Cressex Health Centre and Lynton House Surgery	Sole Controller
Russell Street Surgery (Burghfield and Coley Park)	Sole Controller
Clifton Hampden Surgery	Sole Controller

West Bar Surgery (Banbury Cross Health Centre and Bridge Street Surgery)	Sole Controller
Iron Mountain (UK) Limited	Processor
OASIS Group	Processor
Kelly's Storage	Processor

*Records currently stored with OASIS

**Notes also stored at 3rd Party Provider (Kelly's Storage)

New Patients Records held at Practices that have been Digitised.

Name of Organisation	Role
Banbury Road	Sole Controller
* The Hall Practice	Sole Controller
Simpson Centre and Penn Surgery	Sole Controller
Dr Allan Practice	Sole Controller
The Manor Surgery	Sole Controller
19 Beaumont Surgery	Sole Controller
Swallowfield Medical Practice	Sole Controller
Alchester Group (Victoria House Surgery and Langford Practice)	Sole Controller
Melrose Surgery (Eldon Road)	Sole Controller
Eastfield House Surgery	Sole Controller

*Records currently stored with OASIS

1.5.

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

OASIS utilize a records management system that incorporates document indexing in line with ISO published standards and GDPR. NHS number is entered onto the system for tracking and audit purposes. This enables the subsequent ability to manage, track and monitor each individual medical record. Data capture is completed by OASIS as the supplier.

Following a request by a practice for an archived record to be scanned, all data held within the medical record will be processed, with the supplier transferring individual patient data from one format (paper-based) to another (digital). Once complete the digitised file will be uploaded to the supplier's portal, enabling the practice to access and download.

OASIS upload images to their secure image store on the HSCN network and a Practice will then access the images and download them using the noteSpace desktop application (secure portal)

1.6.

Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)

Clinical Records

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

Reasonable expectations (please specify)

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

Processing the data is necessary to enable the realization of the public benefits listed in 1.2 (e) and is proportionate to that purpose. It is not possible to realize these benefits 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.**

Storage / scanning, tracking and management of medical records.

1.10.**Approximately how many people will be the subject of the processing?**

1000 plus

1.11.**How are you collecting the data?** (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)

Paper form

Choose an item.

Choose an item.

Choose an item.

Choose an item.

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

[Click here to enter text.](#)

1.12.**How will you edit the data?**

The data will not be edited during the indexing or scanning process.

With regard to scanning the data will be transferred from a paper format into an electronic file (text searchable PDF format). Blank pages may not be deleted.

The contents of all LG records will need to be examined prior to the scanning process commencing to ensure that as high a quality image as possible is obtained. There are several non-scannable items which need to be removed which include:

- Staples, paperclips, fasteners etc. taking care not to cause any damage to the original which may affect the capture of information when being scanned.

- Poly pockets / plastic wallets
- Removable media such as CDs and USB hard drives.
- Ensure that any attachments e.g., post it notes; medical results attached to mount sheets, are secured to the page without obscuring information, or are kept with the correct page for scanning so as not to lose the context of the information.

It is the responsibility of OASIS as the supplier to prepare records before they are scanned.

1.13.

How will you quality check the data?

GP Practices: Personal data is also pulled from the existing medical record and therefore the corresponding GP practice is responsible for the accuracy of this data.

OASIS: Upon completion of the transfer of records from Iron Mountain and the corresponding practices, a review is to be held with the supplier and practice to ensure that all the records have been collected, that the data is accurately captured for the full list of records with reconciliation against the practice list. Please refer to the section on “Background Information” detailing the review process.

This will also be the case where all the records are currently stored at the practice’s premises only.

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?

Practice Teams will use the 'noteSpace' desktop application (secure portal) to securely request the return of paper Lloyd George records held in storage with OASIS, the collection of paper Lloyd George records from the Practice and Scan on Demands.

Online face to face training on how to use the noteSpace application is provided to Practices and ongoing support is provided by OASIS’s Client Care Team. Contact details for Client Care will be provided and that Team will for example, be the point of contact for ordering boxes or box barcodes.

Oasis staff have confidentiality clauses in their contract of employment and are planning to introduce anti-bribery training this year.

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).

For specific details please refer to the “Background Information” section above.

Lloyd George records are stored at both the Iron Mountain's warehouse and the corresponding practices. Many records that are stored at Iron Mountain's warehouses have been removed from their envelopes when the records were being scanned by Iron Mountain. In such cases, there will need to be thorough organization and for each record to be placed in a file cover /envelope. These records may be separated by a blank paper or held together with rubber bands.

The level of record reconstruction (if any) will be determined by an initial trial to assess the state of the records stored at by Iron Mountain and the work required. For this trial, an agreed number of items will be transferred to OASIS's site, with both BOB ICB and OASIS project management teams in attendance.

For each load of records received from Iron Mountain, all necessary data fields will be captured upon receipt at OASIS's facility.

Once the data entry is completed, records will be transferred to another of OASIS's facilities for the ongoing physical storage.

Lloyd George Records are collected from corresponding practices and transferred securely to OASIS's storage facility. Indexing is performed whereby the NHS Number is entered into the supplier's records management system, which together with the use of barcodes enables efficient tracking of individual records.

Upon completion of indexing, an inventory of the records will be shared with the practices with a review completed to ensure that the data is captured for a full list of records, with reconciliation against practice lists.

If a request is made by a practice for the retrieval or scanning of a record, the tracking system is used to locate the record, which is then either scanned into electronic format and uploaded to the supplier's portal or transferred securely as a paper file back to the practice, with the transfer of paper files completed through the use of vehicles fitted with an alarm and GPS tracking system, with contingencies in place for accidents and breakdowns during transportation

A project team at OASIS will be responsible for the collection and transfer of records from those practices who were yet to have their notes collected by Iron Mountain. There is also a separate dedicated specialist data entry team. This project team will be responsible for attending each location, packing records according to pre-agreed criteria, and transporting them to the OASIS facility. Data entry of each load for these records will be completed based on the following:

Timescales based on 5 indexers.

> 5,000 list Practice - cataloguing complete 2 working days.

>10,000 list Practice - cataloguing complete 4 working days.

>15,000 list Practice - cataloguing complete 6 working days.

>20,000 list Practice - cataloguing complete 8 working days.

1 indexer = 500 to 750 Patient records per day (type in 10 digit NHS No / place barcode on patient record and scan to box.

This will also be dependent on the additional piece of work / step to place records back into folders.

Speculative - 60 seconds per additional step

Pilot is required to evaluate the extra step.

2.3.**What data/information are you planning to share?**Types Of Information

Archiving / indexing and tracking: Personal Identifiers:

- Name
- Date of birth
- NHS

The above is captured for the initial cataloguing only. NHS number only is retained to enable requests for e.g. delivery to be made by a Practice and for audit purposes.

Scanning: Patient's full medical record, which may include any, some, or all of the following:

- Number
- Name
- Gender
- Address
- Post Code
- Date of Birth/ Age
- Marital Status
- Telephone Number/ Mobile Number
- Email Address
- NHS Number
- NI Number
- Living Habits
- Photographs
- Physical Description
- Online Identifier (IP Address)
- Medical History/ Treatment dates/Diagnosis/Health condition
- Family/ Lifestyle/ Social Circumstance
- Sexual orientation/ Sex life
- Genetic
- Religious/ Philosophical belief
- Racial / Ethnic Origin
- Employment/Career History
- Criminal Proceedings/ Outcomes/ Sentencing
- Offence Committed or Alleged to have Committed

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?

OASIS Group (as the supplier)

2.6.

Why is this data/information being shared?

For the NHSE Lloyd George Digitisation pilot programme, Iron Mountain were successful in the bid to provide the scanning service for Pilot Practices in BOB ICB. Subsequent to the contract award, Iron Mountain failed to deliver the contracted service to the practices. After careful consideration regarding the clinical risks involved, BOB ICB decided to terminate the contract with Iron Mountain and commission another supplier (OASIS) to provide a Records Storage and Management Service.

Through the use of the records management system, which involves the use of indexing (based on personal data fields only) and barcodes, archived records can be located at point of request and either scanned / uploaded to the supplier's portal or transferred securely back to the practice, with the service therefore relying on the sharing of data to enable indexing and the subsequent effective tracking and management of records etc.

2.7.

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

The data is shared directly, noting that the medical records will be held (in storage) by OASIS following collection and the secure transfer from Iron Mountain and the practices (see details in Background Information).

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?

OASIS Group was approved as a Lot 5 (Document Storage, Records Management, and Integrated Solutions) supplier for the NHS SBS Framework, enabling the ICB to contract directly with the provider. The application process requested evidence of accreditation to or compliance with listed standards as required and tested the suppliers' financial and economic standing, technical/professional ability, experience, and status against the industry standards set out in the national specification. In addition to the Data Processing Agreement which is inherent to the provider's contract a Data Sharing Agreement between the practices as Controllers and OASIS will be in place.

2.9.

What reports will be generated from this data/information?

As part of the contract management process BOB ICB will be provided with monthly activity reports detailing the number of records held in storage, new records that have been added, requests for scanned files, retrievals and returns etc. No patient identifiable and only anonymised data will be generated for such purposes.

2.10.

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

No

If yes, are all the right agreements in place?

Choose an item.

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

[Click here to enter text.](#)

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1

Are you proposing to use a third party, a data processor, or a commercial system supplier?

Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.

OASIS Group Head Office, Quadrant 1 Homefield Road, Haverhill, Suffolk, England, CB9 8QP.

OASIS Group Record Centres that could be used for the BOB ICB Project are:

OASIS Group (Winchester) Winnall Down, Alresford Road, Winchester, Hampshire SO21 1FP.

OASIS Group (Swindon) Unit 2 Clearwater Business Park, Frankland Road, Swindon, SN5 8YZ.

OASIS Group (Northampton) Gowerton Road, Brackmills Ind Est, NN4 7BW.

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
OASIS GROUP	Yes	Z1330871
Iron Mountain (UK) Services Limited	Yes	ZA018271
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
OASIS GROUP	OASIS's accreditations include: ISO 9001 – Quality Management System ISO 22301 – Business Continuity Management

	<p>BSI 10008 – Evidential Weight and Legal Admissibility of Electronic Information ISO 14001 – Environmental Management ISO 27001 – Information Security Management BS15713 – Secure destruction of confidential material BS7858 – Screening of individuals working in a secure environment. Cyber Essentials Cyber Essentials Plus</p> <p>Dynamic Purchasing System (DPS) for Digitisation of Lloyd George Medical Records Services, OASIS are approved for Lot 1 – Scanning Services.</p>
OASIS GROUP	<p>ISO 22301 – Business Continuity Management</p> <p>Held at the Winchester Record Centre. <i>BC events are led by the Compliance team and managed by the crisis management and response teams which are based at local sites or within the support services functions which are centralised. Every BC process and procedure which is followed outside of Winchester is aligned to ISO 22301.</i></p>
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
OASIS GROUP	8J050	Standards Exceeded	03/05/2023
Iron Mountain UK plc	8HH60	Standards Met	31/10/2022
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.

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 Lloyd George Records will be held at OASIS's secure warehouse facility, equipped with advanced security, fire protection and environmental controls to safeguard the records. These premises are certified to ISO 9/14/27001 standards.

Personal data, used for indexing / tracking purposes, will be stored electronically in the supplier's records management system, which is ISO 9001 and ISO27001 certified.

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

The data is accessed / controlled electronically by practices via the noteSpace application (secure portal). Access is determined by the Practice Team. It is noted that all suppliers on the national DPS Framework are required to evidence that they meet the required standards around safe and secure handling of data.

Within the storage facilities all doors are intrinsically safe and protected by a door access control system, CCTV and intruder alarms. Entry permissions to different areas are assigned to personnel groups based on their roles on a least privilege basis, thereby managing staff access to office, main warehouse, and vault areas. Access logs are digitally backed up, allowing reports to be generated for audit purposes. A reporting system is in place to delete user access immediately in the event of a lost pass or termination of employment. Each record is indexed and barcoded using specialised data entry software and records management system. OASIS's data entry clerks / staff are assigned unique log in codes enabling control re access and also identification in terms of each movement of a record's history. All vehicles contain dash cams and GPS tracking so that their location can be tracked and monitored at all times, vehicles also have slamlocks, and bulkheads.

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?

Secure storage facility in line with National and ISO 27001 Standards, including that relating to Site Security (i.e. physical security, shutters, CCCTV, alarms, access control, fire detection, fire suppression) and Cyber Security.

Note that all suppliers on the national DPS Framework are required to evidence that they meet the required standards around safe and secure handling of data.

Is a specific System Level Security Policy needed?

[Choose an item.](#)

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 Agreement is inherent to the contact held with OASIS, with BOB ICB responsible for its management.

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).

As part of the NHSE National Lloyd George Digitisation Programme, Practices were asked to display a Privacy Notice (at the Practice and/or website). Privacy Notices are to now be updated to reflect the change to provider / OASIS as a data processor.

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).

The practice is required to respond to individual rights requests as per their usual process and will need to update their procedure with regarding to obtaining information from the Lloyd George record when required.

4.3

How long is the data/information to be retained?

The commissioned service has a contract length dependent on when the National Centralised Storage Solution will be implemented. The agreement with OASIS will be ceased and transferred to the National Solution which is currently in development and is forecast to be in 2 to 3 years (2024/2025) time.

4.4

How will the data/information be archived?

Lloyd George Records will be held in storage boxes, with the OASIS tracking system utilized to locate and retrieve.

OASIS upload the Scan on demand (SCOD) images to their secure image store on the HSCN network and a Practice will then access the images and download them using the noteSpace desktop application (secure portal).

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?

Following the exit process the records will be securely transferred to a determined location, with electronic Personal Data (held on tracking system) to be retained by OASIS for an agreed period of up to 90 days in line with NHS Records Management Code of Practice retention timescales. All personal data is to be deleted from the supplier's system with a certificate of destruction of the data (including back-ups and copies) to be provided for evidential purposes.

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 / processed in a manner that is considered unfair	Possible	Significant	Medium

Risk of data loss due to the transfer of records	Possible	Significant	High
Risk of data loss due to issues identified (i.e. failure to locate records / records forwarded to incorrect practices) / the service currently provided by Iron Mountain	Probable	Significant	High
Highly sensitive data will be processed 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
Risk of information that could cause harm to the patient being disclosed to patient in on demand digital copy of record	Possible	Significant	High
Iron Mountain not fully co-operating with OASIS with the transfer of records and relating information (location of records, etc).	Probable	Significant	High
Patient is adversely affected due to delay in record being returned to practice/added to portal by OASIS	Possible	Significant	Medium

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 / processed in a manner that is considered unfair	Ensure that information relating to the storage of records is made available to patients. 'Privacy notice' for practices to be available on their website and displayed within practice reception area.	Reduced	Low	Choose an item.
Risk of data loss due to transfer of records.	Ensure supplier's transport logistics enable safe and secure movement of records, with robust SOP in place.	Reduced	Medium	Choose an item.
Risk of data loss due to issues identified (i.e. failure to locate	Upon completion of indexing (which is to be completed one practice at a time), an	Reduced	Medium	

records / records forwarded to incorrect practices) / the service currently provided by Iron Mountain	<p>inventory of the records is to be shared with the practices with a review completed to ensure:</p> <ul style="list-style-type: none"> • Data is captured for a full list of records, with reconciliation against practice list • Any discrepancies are identified and rectified together with the practice and with Iron Mountain 			
Highly sensitive data will be processed by a third party	<p>Review of supplier's security accreditations / ensure their completion of DSP Toolkit.</p> <p>Supplier's staff to undertake annual data security training.</p> <p>Storage warehouse is equipped with advanced security and fire protection to safeguard the records - certified to ISO 9/14/27001 standards.</p>	Reduced	Low	Choose an item.
Risk due to lack of compliance / accreditations or adequate data processing contracts in place.	Data processing agreement to be in place with the supplier detailing the nature of the processing alongside the contract.	Reduced	Low	Choose an item.
Access to personal data is unauthorised	<p>Ensure supplier has appropriate security measures / accreditation in place (both physical and cyber).</p> <p>Access is restricted to authorised personnel and must be removed when no longer required.</p>	Reduced	Medium	Choose an item.
Risk of information that could cause harm to the patient being disclosed to patient via on demand digital copy of record	With guidance provided by the ICB / IG Team, GP practice to review and redact any information that could cause harm from the on demand digital copy before disclosing to patient.	Reduced	Medium	Choose an item.

	Digital file to be hidden from online view in patient's electronic record until it has been reviewed and redacted.			
Iron Mountain not fully co-operating with OASIS with the transfer of records and relating information (location of records, etc).	Re-iterating Iron Mountains contractual obligation to co-operate	Reduced	Medium	Choose an item.
Patient is adversely affected due to delay in record being returned to practice/ added to portal by OASIS	Duty of Candour Notice to be displayed on practices' websites Contractual requirement for Oasis to comply with agreed recall process, transfer between sites process and timescales. Duty of candour message to be sent to individual adversely affected patients or displayed on practice website if high number of patients are adversely affected.	Reduced	Low	

5.3**What if anything would affect this piece of work?**

[Click here to enter text.](#)

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?**

Yes

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

OASIS, 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

Practices should review and update their privacy notice. Example text is provided below. Practices that use the SCW privacy notice templates should add this to Appendix A.

Activity	Rationale
Lloyd George Records Storage and Management Service	<p>Purpose – BOB ICB are commissioning and off-site storage solution with a scan-on-demand (SCOD) function.</p> <p>Legal Basis – Article 6(1)(e) ‘...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...’; and</p> <p>Article 9(2)(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</p>

Please note: Good records management supports good data governance and data protection.

When transferring data off site, to use an appropriate form of transport for example secure courier and GP Practices make checks to ensure the information has been received.

Noted from assessment that Oasis – have in place ISO27001, Cyber Essentials plus certification.

Following review by the GP DPO, as BOB ICB DPO am assured risks have been identified and mitigated.

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:

There are no further actions 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 Offsite Archive Storage & Integrated Services (UK) Ltd

Name: [Redacted]

Job Title: Director


Signature: 

Date: 25 September 2023

Signed and approved on behalf of

Name: [Redacted]

Job Title: Data Protection Officer

Signature: 

Date: 27 September 2023

Please note:

Click here to enter text.