Data Protection Impact Assessment (DPIA)

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 should **always** carry out a DPIA where you plan to:

Use **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	✗/✓
Process **special-category data or criminal-offence data on a large scale**;	✗/✓
Monitor a publicly accessible place on a large scale;	✗/✓
Use **innovative technology** in combination with any of the criteria in the European guidelines;	✗/✓
Carry out **profiling** on a large scale;	✗/✓
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	✗/✓
Combine, compare or match data from multiple sources;	✗/✓
Process personal data **without providing a privacy notice** directly to the individual in combination with any of the criteria in the European guidelines;	✗/✓
Process personal data in a way that involves **tracking** individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	✗/✓
Process **children's** personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	✗/✓
Process personal data that could result in a **risk of physical harm** in the event of a security breach.	✗/✓

You as Controller should **consider** carrying out a DPIA where you

Plan any major project involving the use of personal data;	✗/✓
Plan to do evaluation or scoring;	✗/✓
Want to use systematic monitoring;	✗/✓
Process sensitive data or data of a highly personal nature;	✗/✓
Processing data on a large scale;	✗/✓
Include data concerning vulnerable data subjects;	✗/✓
Plan to use innovative technological or organisational solutions;	✗/✓

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

We have written some 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.

CONTENTS

A) BACKGROUND INFORMATION

Describe what you are proposing to do: Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required.	Introduce a new document processing service. No changes to the type of, or manner in which, data is processed, but a change to the platform that is being used to process this data.
Are there multiple organisations involved? If yes – you can use this space to name them, and who their key contact for this work is**.**	Yes – Continuum Health Limited (supplier of Anima), key contact – Rachel Mumford

B) 1. CATEGORIES, LEGAL BASIS, COLLECTION, FLOWS, RESPONSIBILITY

1.1

What data/information will be used? Indicate all that apply.	**Y/N**	**Complete first**
Personal Data	Y	1.2
Special Categories of Personal Data	Y	1.2
Commercially Confidential Information	N	Consider if a DPIA is appropriate
Personal Confidential Data	Y	1.2
Sensitive Data (usually criminal or law enforcement data)	N	1.2
Pseudonymised Data	N	1.2
Anonymised Data	N	Consider at what point the data is to be anonymised
Other (please detail)	N	Consider if a DPIA is appropriate

1.2

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:	
c) The Data Subject has given explicit consent	**N**
Why are you relying on explicit consent from the data subject?	
What is the process for obtaining and recording consent from the Data Subject? How, where, when, by whom.	
Is your consent form compliant with the Data Protection requirements? There is a checklist that can be used to assess this.	
d) It Is necessary for the performance of a contract to which the data subject is party	**N**
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?	

e) It is necessary under a legal obligation to which the Controller is subject	**N**
A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC.	
Identify the legislation or legal obligation you believe requires you to undertake this processing.	

f) It is necessary to protect the vital interests of the data subject or another natural person	**N**
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?	

g) It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller	**Y**
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?	
This processing is carried out in the exercise of official authority in order to provide direct care as per BMA guidance for GP practices as data controllers under the GDPR.	

h) It is necessary for the legitimate interests of the Controller or third party.	**N**
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.	
What are the legitimate interests you have?	

Article 9 (2) conditions are as follows:	
a) The Data Subject has given explicit consent	**N**
Requirements for consent are the same as those detailed above in section 1.2 a).	
b) For the purposes of employment, social security or social protection	**N**
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.	
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	**N**
Requirements for this are the same as those detailed above in section 1.2 d)	
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*

e) The data has been made public by the data subject		*NA*
f) For legal claims or courts operating in their judicial category		*NA*
g) Substantial public interest		**N**
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.		
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		**Y**
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.		
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		**N**
Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available.		

1.3

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

1.4

Confirm whether you will be the Controller and solely responsible for any data processed or will you be doing this jointly with any other organisation?

The Holbrook and Shotley Practice will be the data controller; the supplier will process the data and act as data processor.

1.5

What is the purpose? Describe exactly what is being processed and by whom?

To provide cloud-based storage software for electronic patient documents. This includes letters that the practice receives, scans and uploads to the patient record, as well as letters that the practice receives in an electronic format. This helps the practice to capture, file, workflow, view and manage primary care documents efficiently.

This helps to support the provision of direct care by maintaining accurate patient records within the practice, recording all external documentation and relevant information from other healthcare services in relation to patients is necessary.

Artificial intelligence ('AI') is used in the product to perform some select functions, including to match documents to the correct patient by identifying a patient's name and NHS number from a given document and to identify and suggest potential clinical codes based on the content of the document. Where the AI matches the patient, the Anima platform displays a confirmation message that the patient details have been verified against both the EHR & PDS systems - users can visually acknowledge the match

AI is not used to make diagnoses or automatically action any tasks or next steps, but instead is designed to provide decision support to the end-user, thereby achieving efficiencies and time savings when compared to performing these tasks manually. This involves document data (including patient health data) being processed by Anima's in-house proprietary data model. All data is, as is the case throughout the Anima platform, encrypted in data and at rest, and is stored in the UK.

Coding and actions which are suggested by the AI are accepted/declined, as appropriate, by the user in Anima; once this processing is complete, the document, comments and clinical codes are filed into EMIS/SystmOne.

1.6
Do you owe a duty of confidentiality to any information? If so, specify what types of information. (E.g. clinical records, occupational health details, payroll information)?

The supplier does not have access to the clinical record except as provided via their approved IM1 integration with EMIS/SystmOne. This integration is used to access elements of the patient's medical record within the Anima software, as required by the AI in order to identify relevant clinical information.

The supplier may need to see patient data for strictly limited purposes. For example, this data may need to be accessed to investigate technical problems with the service. These occasions are very rare and only happen when absolutely necessary. Any access to patient information is time-limited and governed by our data processing agreement.

1.7
Are you proposing to use any information for a purpose that isn't direct patient care? Describe that purpose.

No

1.8
Approximately how many people will be the subject of the processing?

Up to the practice list size

1.9
How are you collecting the data?
(e.g. verbal, electronic, paper)

Electronic and paper

1.10
How will you edit the data?

Document content will not be edited; some additional clinical coding and/or commentary may be appended to the document.

1.11
How will you quality check the data?

Data is patient-submitted; reviewing staff will be reminded to use their clinical judgment as would be usual for any other history-taking.

1.12
Review your business continuity or contingency plans to include this activity. Have you identified any risks? If so include in the risk section of this template.

If the service is unavailable, the practice will be able to continue to manually process documents using either alternative software (e.g. the EHR), or by hand.

1.13

What training is planned to support this activity?

Training to be provided by the software provider (at least 1x synchronous training session; supplemented by asynchronous in-app training)

I)	2. LINKAGE, SHARING, FLOWS, AGREEMENTS, REPORTS, NHS DIGITAL

2.1

Are you proposing to combine any data sets?
Detail them here.

No

2.2

What are the Data Flows?
Detail and/or attach a diagram

Documents will be uploaded into Anima via a manual file upload; in the future, documents may also be sent directly into a MESH inbox that can be accessed in the Anima platform. Data is therefore sent to Anima, where the document is processed, and then sent on to the EHR or other final destination of the file.

Anima will intercept MESH messages, by polling the MESH inbox in EMIS/SystmOne. This lets EMIS/SystmOne know that Anima have successfully received the document.

If no poll is sent, it means that Anima have not got the document and EMIS/SystmOne will display it in the same way as documents currently received via MESH. The sender also receives a read/received receipt.

Once the document is in Anima, the user will complete the processing which then delivers the document back into EMIS/SystmOne. This will generate a success/failure message within the user interface of the Anima software for the user filing the document.

2.3

What data/information are you planning to share and who with?

Data will only be shared with registered healthcare professionals to provide direct patient care.

2.4

Why is this data/information being shared and how will you share it?

To ensure that the practice maintains up-to-date information about their registered patients and their active problems and treatment by other healthcare providers. This is necessary to transfer care back to the practice from secondary care and other/fringe services.

2.5

What data sharing agreements are or will be in place to support this?

Data processing agreement is in place with Continuum Health Limited (the manufacturer of Anima). When data needs to be shared with other organisations (e.g. across the PCN or other practices), the appropriate information sharing agreements will be put in place.

2.6

What reports will be generated from this data/information?

In the near future, the Anima software can generate reports on usage; patient data is anonymised and is used only to provide aggregate reporting e.g. on number of documents processed, type of document, source of document.

2.7

Are you proposing to use Data that may have come from NHS Digital? If so are all the right agreements in place?
E.g. SUS data, HES data etc.

Continuum Health Limited (supplier of Anima) have agreements in place with NHS Digital for all applicable systems in use i.e. PDS, GP Connect, IM1 integration.

J)	**3. SECURITY**

3.1

Are you proposing to use a third party, a data processor or a commercial system supplier?
If so use this space to add their details including their official name and address.

Continuum Health Limited, 71-75 Shelton Street, London, WC2H 9JQ

3.2

Is this organisation registered with the Information Commissioner?
Use this space to add their registration details.

Yes (registration no. ZB035442)

3.3

What IG assurances has this organisation provided to you and does the contract contain IG clauses that protect you as the Controller?
E.g. in terms and conditions, their contract, their tender submission.

The organisation will process data on behalf of us as the data controller. We have seen their data processing agreement which clearly delineates the role of data controller and processor and ensures that the supplier is responsible for the data processing that occurs within their network.

3.4

What is the status of their Data Security Protection Toolkit?

R3U6M - Continuum Health Ltd 22/23 Standards met

3.5

How and where will the data/information be stored?

All processor data is securely hosted in Amazon Web Services' EU-West-2 (London) region.

3.6

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

At the practice, data/information is accessed by authenticated users who have been approved to create an Anima account and have attended the relevant training session. The practice also has policies in place to control access, including password- or smartcard-based log-in details for access to IT equipment. The supplier has strict access controls in place to manage staff that are able to view practice data.

3.7

Is there any use of Cloud technology?
If yes you may wish to complete the additional cloud computing questionnaire.

Yes

3.8
What security measures will be in place to protect the data/information? Is a specific Security Policy needed?
E.g. physical, electronic etc. A checklist is available to help you.

All data is encrypted in transit and at rest (AES 256).

3.9
Is any data transferring outside of the UK? If yes describe where and what additional measures are or will be in place to protect the data.
No

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?
Data sharing agreement shared & signed

K)   4. INDIVIDUAL RIGHTS, NOTIFICATION, RETENTION, ACCESS, DELETION, RECTIFICATION, PORTABILITY

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.

Anima may need to be added as a partner supplier/ third party processor to our privacy notice.

4.2
How will this activity impact on individual rights under the GDPR?
Right of access, erasure, portability, restriction, profiling, automated decision making.

Patients will retain their right to access and erasure under the GDPR and can contact the supplier to request the removal of their data.

4.3
How long is the data/information to be retained?

Data submitted through Anima will be retained in alignment with the NHS Records Management Code of Practice (NHS RMCOP) Appendix II. Retention occurs even where the contract with Anima is terminated. Anima will retain a copy of the document and associated audit trail for audit purposes only.

4.4
How will the data/information be archived?

Data will be archived for audit purposes in line with the NHS RMCOP. Access to archived records is restricted and monitored, in accordance with the Destruction of digital records guidance in Section 5.3 NHS RMCOP.

4.5
What is the process for the destruction of records?

Patients can request that any data held by the supplier in relation to them be securely destroyed by the supplier.

4.6
What will happen to the data/information if any part of your activity ends?
In the event of offboarding, requests can be made to the supplier to remove processed data.

4.7
Will you use any data for direct marketing purposes? If yes please detail.
No

L)   5. RISKS, ISSUES AND ACTIVITIES

5.1

What risk and issues have you identified? The DPO can provide advice to help complete this section and approve 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.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, Medium or high
Unauthorised access to personal data	Remote	Significant	Low
Integrity of equipment being used	Remote	Minimal	Low
Malicious use of platform	Remote	Significant	Low
Stored documents are accessed by an inappropriate user	Remote	Significant	Low
AI does not function as expected	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
		Eliminated, reduced or accepted	Low, medium or high	Yes/no
Unauthorised access to personal data	Clinical users must register with their NHS email and clinical accounts are manually verified before being added to ensure that no one who is not registered at a certain practice can access the Anima platform.	Eliminated	Low	Yes
Integrity of equipment being used	All devices used conform to NHS standards for encryption	Reduced	Low	Yes
Malicious use of platform	Restricting the number of reviews a patient account can submit (i.e. if they have a review open, they cannot submit a further request related to the same problem/condition until	Reduced	Low	Yes

	their active request is resolved).			
Stored documents are accessed by an inappropriate user	Best practices followed for storing all documents and photos - data is encrypted in transit and at rest. Access is on an individual basis only authenticated users can view this information.	Reduced	Low	Yes
AI does not function as expected	AI algorithms are rigorously tested. The software development process has multiple tests both manual and automated which are undertaken before any deployment to the production environment. First develop, and then test on the development platform - Deploy to the internal pre-production environment for further user testing before releasing it to production.	Reduced	Low	Yes

5.3
Do you know of anything that will have an effect on this piece of work?

No

5.4
Do you have any further comments to make that do not fit elsewhere in the DPIA?

N/A

M)	**7. DATA PROTECTION OFFICER COMMENTS AND OBSERVATIONS**

7.1 **Comments/observations/specific issues**	
DPO date and signature	

N)	**8. OUTCOME ASSESSED BY PRACTICE**

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:
(delete all that do not apply)

    a) There are no further recommendations that need action.
    b) There are further recommendations that need action and they are:
    c) We should not proceed at present because:

We believe there are
(delete all that do not apply)

    a) No unmitigated or identified risks outstanding

b) Risks that need further consideration and management *(list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below)*

c) Considerable risks that need further consultation with the ICO *(list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below)*

Remaining risks and nature of potential impact on individuals in outcome b and c above.	Likelihood of harm	Severity of harm	Overall risk
Include associated compliance and corporate risks as necessary.	Remote, possible or probable	Minimal, significant or severe	Low, Medium or high

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above - b and c				
Risk (from box above)	Actions to be taken	Effect on risk	Residual risk	Measure approved
		Eliminated, reduced or accepted	Low, medium or high	Yes/No

Signed and approved on behalf of **Caldicott Guardian or IG Lead**

Name: Dr Jonathan D'Souza

Job Title: Partner GP and Caldicott Guardian

Signature: JDS   Date: 07/07/2025

Signed and approved on behalf of **by Project Lead**

Name: Jane Murray

Job Title: Practice Manager

Signature: JWM   Date: 07/07/2025

Please note:

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

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