Data Protection Impact Assessment (DPIA) Template

Under the Data Protection Act 2018 (DPA) A DPIA should be completed at the start of any major project involving the use of personal data.

Consideration must also be given to all other applicable laws concerning privacy, confidentiality, or the processing of personal data , including the Human Rights Act 1998, the Health and Social Care Act 2015, the Common Law Duty of Confidentiality (based on case law) and the Privacy and Electronic Communication Regulations amongst others.

It is designed to detail the processes and identify any risks to data before the project begins.

The outcome may affect the project plan and changes may need to be made.

A DPIA should always be completed:

1. when processing special-category data (health data) or sensitive data
2. processing personal data that could result in a risk of physical harm in the event of a security breach

and considered:

3. in any project involving the use of personal data
4. if the processing includes data concerning vulnerable individuals
5. planning to use innovative technological or organisational solutions

BACKGROUND INFORMATION	
Date of completion:	25.11.24
Name of project	Heidi AI – transcribing software
Name of the GP Surgery	Alma Road Surgery
Who has prepared this DPIA/ Practice lead?	Dr Jabir Merali
Who is your Data Protection Officer?	Caroline Sims
Describe what you are proposing to do: Give the aims of the project and the general process involved.	The practice plan to use Heidi AI – standalone software -to support clinicians in writing clinical records by transcribing clinician consultations, and documents. Heidi is an AI scribe system which will learn the natural language of the users, and categorise the data into the appropriate sections of the electronic patient record. The resulting record can be integrated into the clinical system
Which other organisations are involved? Detail the other organisations involved and who is their main contact?	Heidi Health https://www.heidihealth.com/uk

What is the legal basis for processing this data in this activity?

Article 6 (1) of the GDPR includes the following:	
a) The Data Subject has given explicit consent	Y
This should not be the only legal basis for processing the data.	
b) It Is necessary for the performance of a contract to which the data subject is party… This does not mean the NHS Contract but a contract with an individual such as an employment contract.	N
c) It is necessary under a legal obligation to which the Controller is subject Such as sending employee salary information to HMRC, providing information on Covid vaccinations etc.	N
d) It is necessary to protect the vital interests of the data subject or another natural person Such as in emergency care, safeguarding or other matter of life and death.	N
e) It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller This is commonly used for delivering NHS contracts, the processing must be a targeted and proportionate way to obtain the data being used. *This is to analyse and develop future support for GP consultations and patients mental health*	Y
f) It is necessary for the legitimate interests of the Controller or third party. This would only apply if the legitimate interest is in addition to and not the normal NHS contact or public authority.	N

When **special category data** is being processed in addition to the lawful basis in Article 6.1 a separate condition for processing must be present from Article 9.2 conditions are as follows – do not select items d,e,or f.

a)	**The Data Subject has given explicit consent**	**Y**
b)	**For the purposes of employment, social security or social protection**	**N**
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**
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**
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**
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**

Are you the data controller, and will any other organisation be joint or individual data controllers?.

Name of organisation	Individual, joint controller or processor.
Surgery J82	Data controller
Heidi Health - AI	Processor

Describe exactly what is being processed and by whom?

Consultation recording by Heidi Health AI and then processing into medical record for practitioner to approve and amend before filing into the record.

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)?

Yes – clinical records and patient identifiable information.

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

No

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

15821

How are you collecting the data and can it be edited?
(e.g. verbal, electronic, paper)

Electronic – Patient data can only be edited by the practice.

What are the data flows for this processing? *Provide detail for the actual process involving the practice.*
The clinician will identify the patient before they activate Heidi. All conversations within the consultation will then be picked up by Heidi and transcribed into the record. The GP will quality check the consultation is a fair reflection before saving to the patient's medical record.

What personal data will be shared and how?
The following patient data items may be recorded and transcribed by Heidi:

- Name
- Address
- Phone number
- Gender
- Sexual orientation
- Date of birth
- Relationship status
- Family and social history
- Medical history
- Progress notes
- Medications & prescriptions
- Allergies
- Diagnosis status
- Lab orders & results
- Disability

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

Contract with Heidi Health

What reports will be generated from this data/information?

Random periodic quality control and accuracy audits may be carried out.

3. DATA SECURITY

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

Are all organisations involved registered with the Information Commissioner?
Use this space to add their registration details.

J82xxx xxx Surgery Z6615285
Heidi health Trading Pty Ltd ZB671518

How will data be stored?

Within the existing clinical system and as pseudonymised data with Heidi Health on UK servers.

What IG assurances have the other organisations achieved? i.e. Cyber Essentials Plus, ISO27001 etc.
Cyber Essentials

ISO 27001

DTAC

Do all organisations complete the Data Security Protection Toolkit, what is the status of their last submission?

J82xxx Xxxxx Surgery Standards Met 2023-24

I7D4H Heidi Health Ltd Standards met 2024-25

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

This is available for clinicians to use as part of their normal consultations. Access to the clinical record is by RBAC code and smartcards for all staff.

Is there any use of Cloud technology? What Cloud servers are used?

Heidi is a healthcare IT system, specifically a cloud-based artificial intelligence medical scribe platform hosted on UK servers

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

In addition to the security shown above Heidi determines the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions. Permissions and access rights not expressly granted shall be, by default, prohibited. Heidi’s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorised party.

Do All staff involved in processing undertake annual Data Security and protection training?

Yes

Is any data transferring outside of the UK?

No

Embed a copy of the Data Sharing Agreement for this processing.

Have you added this to your privacy notice Appendix A?

Yes

How long is the data/information to be retained?

Records are retained in accordance with the NHS Records Management Code of Practice 2021

What is the process for the destruction of records?

Data is stored temporarily and deleted once processing is completed.

What will happen to the data/information if any part of your activity ends– if the patient decides to withdraw consent to sharing?

N/A

Confirm that this data will not be used for direct marketing purposes? If No please detail.

Confirmed

RISK ASSESSMENT

Enter the potential risks to the data and impact on the individuals involved.

Describe the 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
Access of Heidi data by unauthorised individuals	remote	significant	low
GP name individuals in the dictation	Possible	Significant	Medium
Speech to text fails to accurately transcribe terminology or drug names	Possible	Significant	Medium

5.2

Describe any actions you can take to minimise or eliminate the above risks.

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, medium or high	Yes/No
Access of Heidi data by unauthorised individuals	All access is controlled by practice and Heidi Health by role based access codes.	reduced	Low	
GP name individuals in the dictation	Clinicians must be careful when dictating not to name the patient or other individuals. The transcript should be checked before filing is completed.	reduced	Low	
Speech to text fails to accurately transcribe terminology or drug names	The transcript must be checked before completing the filing for any errors and omissions.	reduced	Low	

5.4

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

Heidi Data Privacy
Impact Assessment

6. CONSULTATION

Have any other organisations been consulted or given approval for this processing?

N/A

7. DATA PROTECTION OFFICER COMMENTS AND OBSERVATIONS

7.1 **Comments/observations/specific issues**	The potential risks from the dictation and understanding of the AI system should reduce in use. The clinician using Heidi must check the transcript before it is filed to the patient record to ensure that it has no errors. I am happy for this to proceed as a useful element to the clinician's day to day work in supporting patient care. The practice must add this to the privacy notice, website and their data flow map (IAR)
DPO date and signature	Caroline Sims 10/1/2025

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.

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

a) No unmitigated or identified risks outstanding

Remaining risks and nature of potential impact on individuals in outcome b and c above. 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

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 XXX Surgery **Caldicott Guardian or IG Lead**

Name:

Job Title: Managing Partner / IG Lead

Signature: Date: 2025

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

Name:

Job Title: Partner

Signature: Date: 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: