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:	13.1.25
Title of the activity/processing:	Rapid Health AI
Name of the GP Surgery	
Who has prepared this DPIA/ Practice lead?	
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.	Use Rapid Health AI as a triage assist tool to book appointments. It is on our website, and we also direct patients to use it by our reception team. It is easier for patients to book appointments directly and eases the workload on reception and telephones.
Which other organisations are involved? Detail the other organisations involved and who is their main contact?	Rapid Health AI (support@rapid health.co.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.
Surgeries	Inidividual
Rapid Health AI	Processor

Describe exactly what is being processed and by whom?

Patients will use Rapid Health AI to input their details and health issue and it will then direct them to appointment bookings. Patients add their details on the Rapid Health website. It does check details to make sure the patient is matched correctly. We have many appointments lots created of different types. It does inform the patient if there are none available. If they are not happy with their outcome, they contact our reception team to discuss it.

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.

Rapid Health checks each patient and if the details don't match, they can go no further. If it did match to the wrong patient, our reception team can sort this with EMIS and we can contact rapid Health directly to correct their system.

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?

16604

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

Electronic and it cannot be edited

What are the data flows for this processing? *Provide detail for the actual process involving the practice.*
Processed through Rapid Health AI into their inbox online and then reception action them by logging into the Rapid Health inbox online and then save them into EMIS.

What personal data will be shared and how?
Any medical details the patients choose to put onto their enquiry. It will also share individual demographics of patients

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

EMIS approved partner

What reports will be generated from this data/information?

Only psuedonymised or anonymised statistical data for figures on patient usage

3. DATA SECURITY

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.

Rapid Health Ltd 2024
86-90 Paul St
London
EC24 4NE

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

Rapid Health Ltd ZA620101

How will data be stored?

AWS servers in UK

What IG assurances have the other organisations achieved? i.e. Cyber Essentials Plus, ISO27001 etc.
Rapid Health Ltd – Cyber Essentials Dec 2024-25

ISO 13485 conformity

DCB 0129 Clinical Risk Management Standard

DTAC passed

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

9KG49 Rapid Health Standards Met 2023/24

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

RBAC access to clinical system

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

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

Rapid Health data is encrypted at rest and in transit via HTTPS to TLS1.3

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

Is any data transferring outside of the UK?

Sometimes organisations and individuals who work for Rapid Health may manage information outside the EEA. In those circumstances they will ensure we have a valid reason under current data protection legislation to do so. This could include ensuring the country or organisation where the data is held has been approved as having adequate data protections standards by the UK and EU.

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

Have you added this to your privacy notice Appendix A?

No, this will be done when approved

How long is the data/information to be retained?

Rapid Health hold your information for a period of up to seven years from the end of your relationship with RAPID HEALTH or its services, in line with our retention and disposal policy.

What is the process for the destruction of records?

Rapid Health Data Protection Pack.pdf

See section 11 of the Protection Pack for GP Practices

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

The information stored on the patient medical record will remain. Information held by Rapid Health will be deleted in line with their retention protocol

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** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, Medium or high
Incorrect data being matched to the wrong patient	remote	minimal	low

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
Incorrect patient data matched	Rapid Health AI checks each patient and does match if all details are not correct. If an error were to happen, we would inform Rapid Health immediately and remove the entry from our records.	R	L	Yes

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

No

6. CONSULTATION

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

No

7. DATA PROTECTION OFFICER COMMENTS AND OBSERVATIONS

7.1 **Comments/observations/specific issues**	This is designed for the NHS to support patient care and offer a faster booking service to patients. The company has good security and adheres to UK data protection requirements. The risks are minimal as the patient enters their own information at the start. I am happy for this to proceed.
DPO date and signature	Caroline Sims 19/2/2025

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.
~~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. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** 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** Eliminated, reduced or accepted	**Residual risk** Low, medium or high	**Measure approved** Yes/No

Signed and approved on behalf of {insert name of organisation} **Caldicott Guardian or IG Lead**

Name: ……

Job Title: ……

Signature: …….. Date: …….

Signed and approved on behalf of {insert name of organisation} **by Project Lead**

Name: ……

Job Title: ……

Signature: …….. Date: …….

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: