PRIVACY IMPACT ASSESSMENT

Privacy impact assessments (PIAs) are tools which can help organisations identify the best (and most effective) methods to stay compliant with data protection obligations, and to ensure they can protect individuals' privacy.

The practice's designated Data Controller must carry out PIAs where the type of data processing is likely to result in an elevated risk of affecting the privacy, rights and freedoms of individuals. They can be used when starting a new project, implementing a new process, or making changes to a process.

The blue comments in the sample document below provide advice on how to fill out the form.

QUESTION	RESPONSE							
Will this project/system/process/change contain any person identifiable data?	**No**		**Patient**		**Staff**		**Other**	
If the answer is NO, then a Privacy Impact Assessment is not required.	**If other, please specify;**							
The purpose for the collection of data	Treatment of patients							
Does the new this project / system / process / change include security to protect privacy of data?	Yes							

What data information will be held on the system(s)?

Tick all that apply

Sensitive				Personal			
Name	y	Next of Kin	y	Sex	y	Medical History	y
Address	y	Hospital No.	y	Religion	y	Treatment	y
Postcode	y	NHS No.	y	Occupation	y	Ethnicity	y
DOB	y	Nat Ins no.	y	Diagnosis	y	Staff data	y
Sex	y	Consultant	y	**Other**			
GP	y						
Other							

Will this project / system / process / change collect any new personal data that has not been collected before?		**YES**	If YES, please provide details of the data being collected:

QUESTION	RESPONSE
What checks have been made regarding the reasons for collecting the data?	*There is a need to collect this date in order for this GP practice to care for all patients under the current NHS Contract*
Does this project / system / process / change involve new or adapted data collection protocols that do not clarify the reasons or methods of collection?	**Yes, it is in English and visible for patients to see on: Website, TV screens, within Waiting room**
Is the third party contract/supplier of the system registered with the Information Commissioner?	EMIS
Has the 3rd Party supplier completed and IG Toolkit?	Yes
Does the contract with the 3rd Party contain all the necessary IG clauses (including DPA and FoI)?	Yes
Does this project / system / process / change comply with privacy laws?	Yes
Who will be providing the information?	Patient, Employees, other practices, this practice secondary care providers
Do you need consent from the above to enable you to lawfully process person identifiable data? If so, how will you obtain consent?	No

Have individuals been informed of and given consent to processing their data?	Implied Consent due to: Performance of contract, Legal Obligation, Vital Interest of the data subject, Public interest, Legitimist interest – for the business we do
How will you keep the information current and up to date?	Will there be a review of recorded consent to ensure it has been updated?

Who will have access to the data?	All employees of this practice.										
Will there be an audit trail in place for this project / system / process / change?	Yes. clinical systems, web-based logins										
What assessment has been done to ensure processing sensitive data will not cause harm or damage to the individuals concerned?	GDPR, Information Governance training for all employees										
What are the retention periods for this data?	Data will not be removed or destroyed.										
How will the data be destroyed when it reaches the end of its retention period?											
Will this information be shared with anyone else? Will it involve more than one organisation?	Yes. NHS organisations have access to this data										
Where will the information be stored or accessed in the practice? Tick or state in 'Other' section	On Paper		Database saved on network drive		Website		Dedicated IT System (Secured)	Y			
	Other (Please state)										
How will the information be transported?	*NHS Mail*		*3rd Party Email*		*Website*		*Fax*				
	Telephone		*Courier*		*Hand delivered*		*Post (internal)*				
	Post (External)		***Other: (No transportation)***								
Are there safeguards and/or procedures in place to recover data which may be damaged through the following;	Human Error	YES			Cyber-attack / Virus	YES					
	Network failure	YES			Theft	YES					
	Fire/water damage	YES			Other damage	YES					
	Provide a copy of policies or procedures for the above										

Do you have a continuity plan/contingency for any unforeseen events?	YES		Provide a copy of your Business Continuity Plan
Is there an Information Security Management process/policy in place?	YES		Provide the policy titles of the related documents
Will you be transferring any data outside the European Economic Area (EEA)?			If yes, please state the destination below;
	NO		
Please describe the data being transferred to any non-EEA destination.			