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? **If the answer is NO, then a Privacy Impact Assessment is not required.**	**No** ☐ **Patient** ☐ **Staff** ☐ **Other** ☐ **If other, please specify;**
The purpose for the collection of data	*e.g. research, audit, treatment*
Does the new this project / system / process / change include security to protect privacy of data?	*e.g. any security software, encryption, pseudonymisation, anonymization, high level authentication*

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

Tick all that apply

Sensitive				Personal			
Name	☐	Next of Kin	☐	Sex	☐	Medical History	☐
Address	☐	Hospital No.	☐	Religion	☐	Treatment	☐
Postcode	☐	NHS No.	☐	Occupation	☐	Ethnicity	☐
DOB	☐	Nat Ins no.	☐	Diagnosis	☐	Staff data	☐
Sex	☐	Consultant	☐	**Other**			
GP	☐						
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?	*E.g. Is it relevant? Are the methods sufficiently safe and secure? Is there a need for this data in particular?*

Does this project / system / process / change involve new or adapted data collection protocols that do not clarify the reasons or methods of collection?	**Yes or No** *E.g. does the collecting of data have a clear and understandable explanation of how the data is collected?* *Is it in plain English, or have a process map that clarifies how it collects the data?*
Is the third party contract/supplier of the system registered with the Information Commissioner?	(Enter supplier's IC notification no. here)
Has the 3rd Party supplier completed and IG Toolkit?	
Does the contract with the 3rd Party contain all the necessary IG clauses (including DPA and FoI)?	
Does this project / system / process / change comply with privacy laws?	E.g. Data Protection Act, Freedom of Information, Privacy and Electronic communications Regulations 2003.
Who will be providing the information?	e.g. Patient, employees, other company
Do you need consent from the above to enable you to lawfully process person identifiable data? If so, how will you obtain consent?	State whether consent is needed and how you will obtain it, e.g. written consent from patients / staff, signed consent review. State how you will get consent and how it will be recorded. Also include an option for people not to give consent, e.g. tick box saying "I do not consent to provide this information etc."

Have individuals been informed of and given consent to processing their data?	Have they turned down consent, have they provided implicit or explicit consent? (Implicit is implied e.g. leaflets; explicit could be a signed form or verbal consent)
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? E.g. an annual letter to patients/staff to review the consent provided.
Who will have access to the data?	Who will have/need access to the information, and in what manner? E.g. How do you record Clinical Systems, spreadsheets, paper records, sign-in/sign-out sheets,

	Security request forms for logins etc.											
Will there be an audit trail in place for this project / system / process / change?	E.g. Access to clinical systems will need users to use a smartcard. Sign-in/sign-out sheets, IT logs for access to Open Exeter, 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?	What assessment was carried out to ensure processing the data does not endanger or discredit the subjects, and it will remain confidential?											
What are the retention periods for this data?	Timescales for keeping data types can be found in the NHS Codes of Practice (Records Management)											
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?	Will other NHS organisations have access to this data (e.g. Trusts)? IF external organisations have access to the data, then state how the data will be transferred or accessed, and how it will be kept secure.											
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)					
	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:***									
Are there safeguards and/or procedures in place to recover data which may be damaged through the following;	Human Error	YES		NO		Cyber-attack / Virus	YES		NO			
	Network failure	YES		NO		Theft	YES		NO			
	Fire/water damage	YES		NO		Other damage	YES		NO			
	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
	NO		
Is there an Information Security Management process/policy in place?	YES		Provide the policy titles of the related documents
	NO		
Will you be transferring any data outside the European Economic Area (EEA)?	YES		If yes, please state the destination below;
	NO		
Please describe the data being transferred to any non-EEA destination.			