The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at Blake House Surgery.

Step 1 – Determining the need

DOES THE PROCESS INVOLVE ANY OF THE FOLLOWING:	YES	NO
The collection, use or sharing of existing data subjects' health information?		
The collection, use or sharing of additional data subjects' health information?		
The use of existing health information for a new purpose?		
The sharing of data subjects' health information between organisations?		
The linking or matching of data subjects' health information which is already held?		
The creation of a database or register which contains data subjects' health information?		
The sharing of data subjects' health information for the purpose of research or studies (regardless of whether the information is anonymised)?		
The introduction of new practice policies and protocols relating to the use of data subjects' personal information?		
The introduction of new technology in relation to the use of data subjects' personal information, i.e. new IT systems, phone lines, online access, etc?		
Any other process involving data subjects' health information which presents a risk to their "rights and freedoms"?		

If the answer is yes to one or more of the above questions, a DPIA is required; proceed to Step 2.

Step 2 – Assessing the risks

Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

What information is being collected and how?

Where is the information being collected from and why?

How often is the information being collected?

Information use – Is the data obtained for specified, explicit and legitimate purposes?

What is the purpose for using the information?

When and how will the information be processed?

Is the use of the information linked to the reason(s) for the information being collected?

Information attributes – Personal data shall be accurate and, where necessary, kept up to date

What is the process for ensuring the accuracy of data?

What are the consequences if data is inaccurate?

How will processes ensure that only extant data will be disclosed?

Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

What security processes are in place to protect the data?

What controls are in place to safeguard only authorised access to the data?

How is data transferred; is the process safe and effective?

Data subject access – Personal data shall be accurate and, where necessary, kept up to date

What processes are in place for data subject access?

How can data subjects verify the lawfulness of the processing of data held about them?

How do data subjects request that inaccuracies are rectified?

Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Will information be shared outside the practice; are data subjects made aware of this?

Why will this information be shared; is this explained to data subjects?

Are there robust procedures in place for third-party requests which prevent unauthorised access?

Retention of data – Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

What are the retention periods associated with the data?

What is the disposal process and how is this done in a secure manner?

Where is data stored? If data is moved off-site, what is the process; how can data security be assured?

Step 3 – Risk mitigation

Information collection – The risk

Personal data is collected without reason or purpose – increased risk of disclosure.

Information collection – The mitigation

The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected.

Information use – The risk

Personal data is used for reasons not explained to, or expected by, the data subjects.

Information use – The mitigation

Clearly explain and display to data subjects how their information will be used. Data-sharing requires a positive action, i.e. opting in, not opting out!

Information attributes – The risk

Data is inaccurate or not related to the data subject.

Information attributes – The mitigation

Make sure robust procedures are in place to ensure the data held about data subjects is accurate, up to date and reflects the requirements of the data subject for which it was intended.

Information security – The risk

Unauthorised access to data due to a lack of effective controls or lapses of security/procedure.

Information security – The mitigation

Ensure that staff are aware of the requirement to adhere to the practice's security protocols and policies; conduct training to enhance current controls.

Data subject access – The risk

Data subjects are unable to access information held about them or to determine if it is being processed lawfully.

Data subject access – The mitigation

Ensure that data subjects are aware of access to online services and know the procedure to request that information held be amended to correct any inaccuracies.

Information disclosure – The risk

Redacting information before disclosure might not prevent data subjects being identified – i.e. reference to the data subject may be made within the details of a consultation or referral letter.

Information disclosure – The mitigation

Make sure the policy for disclosure is robust enough to ensure that identifying information is removed.

Retention of data – The risk

Data is retained longer than required or the correct disposal process is not adhered to.

Retention of data – The mitigation

Ensure that practice policies and protocols clearly stipulate data retention periods and disposal processes. Review and update protocols and policies and, if necessary, provide training for staff to ensure compliance.