Haydock Medical Centre

Data Protection Impact Assessment Procedure
Version No: 1

The purpose of the Data Protection Impact Assessment Procedure is to support the 7 Caldicott Principles, the 10 Data Security Standards, General Data Protection Regulation (2016), Data Protection Act (2018), the common law duty of confidentiality and all other relevant legislation. Data Protection is a fundamental right and the Practice will embrace the principles of data protection by design and default.

Document type	Data Protection Impact Assessment Procedure
Date approved	30/06/21
Date implemented	30/06/21
Next review date	August 2021 or sooner should legislative change require.
Policy author	Mid Mersey Digital Alliance IG Team
Applies to	All Staff

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled", as they may not contain the latest updates and amendments. For the avoidance of doubt please see the Practices Information Governance Lead.

Contents Page

1.0 Introduction

The General Data Protection Regulation (GDPR) introduces a new obligation and Haydock Medical Centre is expected to carry out a DPIA before implementing new changes or processing that are likely to result in high risk to individuals' interests.

A DPIA should be carried out whenever there is a change that is likely to involve a new use; or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset is being introduced.

This document is a practical tool to help identify and address privacy concerns at the design and development stage of a project. Carrying out a DPIA will assist the Practice in systematically and comprehensively analysing all processing, helping to identify and minimise privacy risk.

It is important for the Practice to carry out a DPIA before a new system or process is implemented as failure to identify and mitigate privacy risk is required by the General Data Protection Regulations (2016).

2.0 Scope

The Practice is committed to adhering to the 10 National Data Security Guardian Standards (NDG) in order to ensure the protection and security of all Data which is processed, shared, stored and transferred in and out of the Practice.

This guidance note/procedure was created in conjunction with the advice from the Information Commissioner's Office following the General Data Protection Regulation (GDPR) which came into force on 25th May 2018.

This document applies to all staff, whether permanent, temporary or contracted and all staff are required to familiarise themselves with the Practice DPIA procedure. This document also applies to all third parties authorised to undertake work on behalf of Haydock Medical Centre

3.0 Purpose

This document/procedure will assist Haydock Medical Centre members of staff to understand the benefits of carrying out a DPIA and also set out the procedures for the Practice and staff to follow when implementing new changes.

Performing a Data Protection Impact Assessment should be considered in the following circumstances:

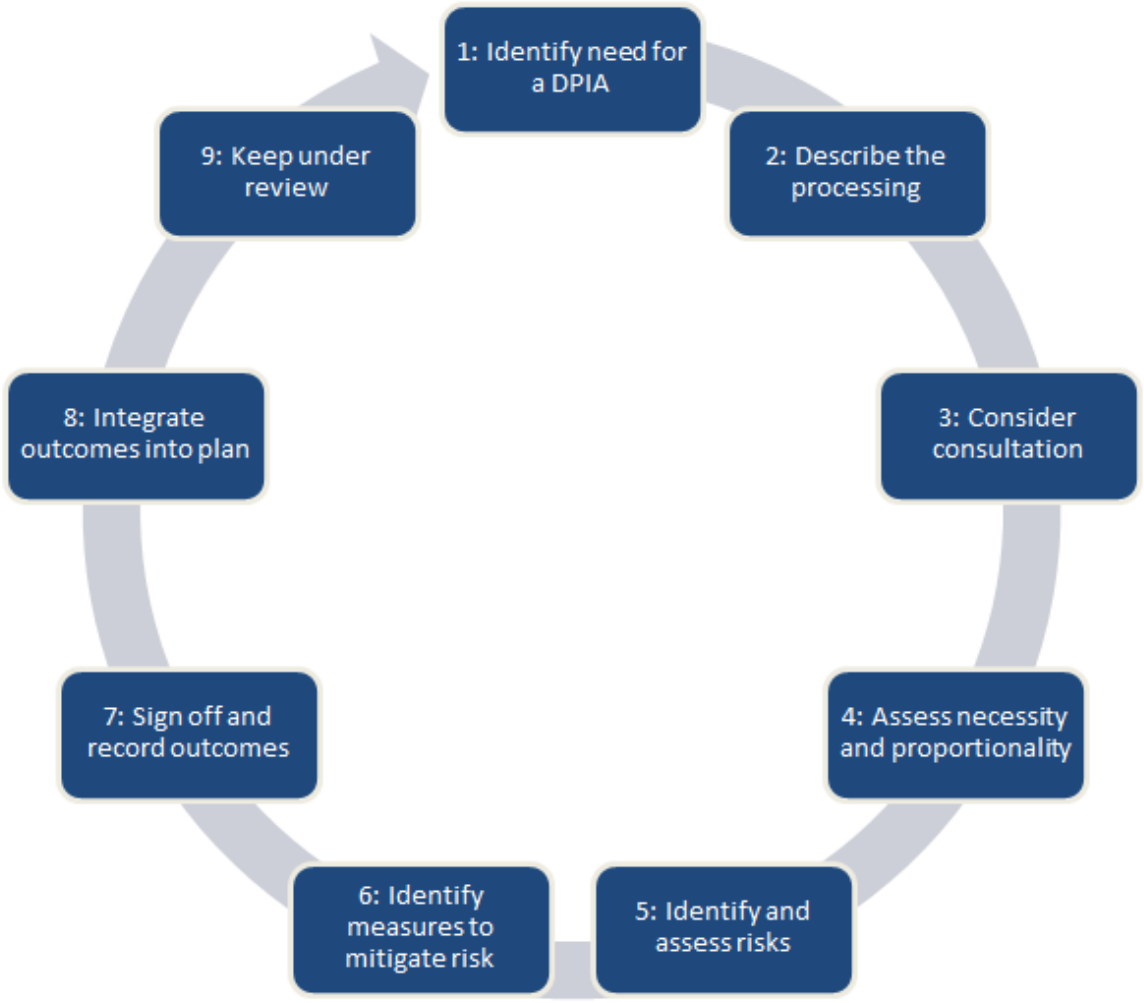
- Introduction of a new paper or electronic information system to collect and hold personal data.
- Update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information.
- Changes to an existing system where additional personal data will be collected.
- Proposal to collect personal data from a new source or for a new activity.
- Plans to outsource business processes involving storing and processing personal data.
- Plans to transfer services from one provider to another that include the transfer of information assets.
- Any change to or introduction of new data sharing agreements.

4.0 Key Roles And Responsibilities

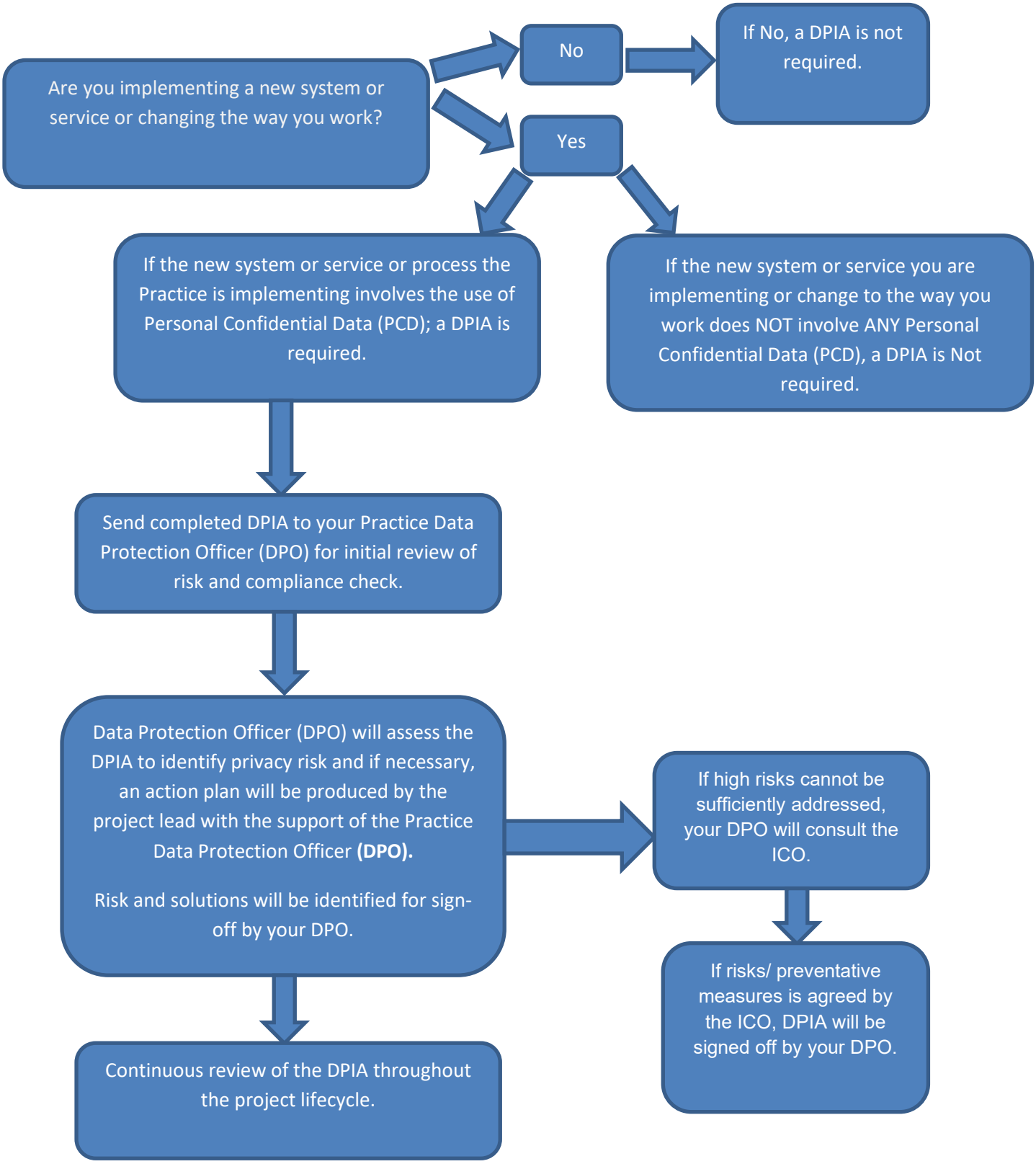
Role	Responsibility
Caldicott Guardian/Senior GP Partners	The Caldicott Guardian/ Senior GP Partners have the ultimate responsibility for ensuring that there are adequate standards for protecting patient information, ensure the Practice carries out a DPIA when implementing new changes or process, ensure that privacy risk are identified and measures are put in place to mitigate identified risk.
Practice Managers/IG Leads	Practice Managers /IG Leads are responsible for ensuring all staff are familiar with the DPIA procedure and have suitable access to this document.
All Staff	Have a responsibility to: • Familiarise themselves with the Practice DPIA procedure. • Identify privacy risk associated with any assets at the Practice. • Log/report near misses/data breach to the Practice Managers.
Data Protection Officer	The DPO has responsibility for Data Protection compliance: The DPO role for Haydcok Medical Centreis fulfilled by Name to be confirmed St.Helens IG team

5.0 Step To Follow

Haydock Medical Centre will carry out a DPIA at the beginning of a project life cycle, in order to address all privacy concerns and risk. The Practice will adhere to the flow chart below;



APPENDIX 1: Data Protection Impact Assessment Procedure



Appendix 2: Data Protection Impact Assessment Checklist

This document must be completed for any new system, application or change in service which involves personal identifiable information. It must be completed as soon as the new service / or change is identified by the Project Manager / System Manager or Information Asset Owner.

There are 2 types of Data Privacy Impact Assessments – a small scale and full scale. This proforma is based on the Small Scale DPIA. Following completion of this proforma, it may be necessary to conduct a Full Scale DPIA. Full details are available in the Information Commissioner's handbook.

Section A: New/Change of System/Project General Details

Name:		
Objectives:		
Background: (Why is the new system/change in system required?)		
Benefits:		
Risk:		
Information Asset Owners (All systems/assets must have information Asset Owner (IOA). IAO's will be the Practice Manger or Partner GP	Name:	
	Title:	

	Department	
	Telephone	
	Email:	
Date PIA was completed		

Section B Privacy Impact Assessment Key Questions

Please complete all questions with as much detail as possible.

Further guidance on specific items can be found on the Information Commissioner's website.

Click here

Question	Response
Will the new system or application contain Personal Identifiable Information? If answered 'No' you do not need to complete any further questions as a PIA is not required.	☐ No ☐ Patient ☐ Staff ☐ Other (please specify)
Please state Purpose Purpose for the collection of the data : i.e. patient treatment , health administration, research, Human Resources, contractors information, etc	
Please tick the data items that are held in the system? Personal Sensitive	☐ Name ☐ Address ☐ Post Code ☐ Date of Birth ☐ GP ☐ Consultant ☐ Next of Kin ☐ NHS Number ☐ NI Insurance ☐ Treatment Dates ☐ Sex ☐ Diagnosis ☐ Religion ☐ Occupation ☐ Ethnic Origin ☐ Medical History Other please state here :
Will the asset collect new personal and sensitive data which have not	☐ Yes ☐ No

been collected before?	
Do you plan to gain the consent of the individuals concerned prior to the system being implemented?	☐ Yes ☐ No
If yes how will that consent be obtained?	
Have the individuals been informed of and given their consent to all the processing and disclosures?	☐ Yes (explicit) ☐ Yes (implicit in leaflets, website etc) ☐ No
What checks have been made regarding the adequacy, relevance and necessity for the collection of sensitive / personal data for this project / service?	
Has the third party contract / supplier of the system registered with the Information Commissioner? What is their notification number? Name and Address details of the third party contractor/supplier	☐ Yes ☐ No Number ……
Does the third party / supplier, contracts contain all the necessary Information Governance clauses including information about Data protection and Freedom of Information?	☐ Yes ☐ No
Is there a Sharing Agreement in place?	☐ Yes ☐ No
Is the Project compliant with the Data Protection Act 1998?	☐ Yes ☐ No
Who provides the Information?	☐ Patient ☐ Staff ☐ Others – Please specify e.g. Interfaces with EMIS/System One ☐ Third Party
Will the Information be kept up to date? How will the personal data be checked for accuracy? Who will be responsible for checking	☐ Yes ☐ No Please Specify – Please Specify -

the accuracy?	
Who will have access to the information?	
Can the data be easily obtained by data Subject upon request?	☐ Yes ☐ No
Do you plan to send direct marketing messages by electronic means? This includes both live and pre recorded telephone calls, fax, e mail, text messages or via social networking sites?	☐ Yes ☐ No Please Specify -
If applicable, are there procedures in place for an individual request to prevent processing for purpose of direct marketing in place?	☐ Yes ☐ No
Is there a useable audit trail in place for the system if applicable? For example to identify who has accessed a record?	☐ Yes ☐ No
Is automated decision making used? If yes, how do you notify the individual? Can there be any human intervention if required?	☐ Yes ☐ No Please Specify - ☐ Yes ☐ No
What are the retention periods for this data and have they been documented? (Please refer to the Records Management Code of Practice for Health and Social Care)	☐ Yes ☐ No
How will the data be destroyed after it is no longer necessary?	
Will the information be shared with other organisation? By what means will the information be shared?(e.g. post, emails, fax etc.) (if yes how will the data be sent/accessed and secured)	☐ Yes ☐ No If yes, please Specify – Please Specify - Please Specify -
Are you transferring any personal and/or sensitive data outside the EEA?	☐ Yes ☐ No

If Yes Where?	Please Specify -
Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	
Are there Security Management Policies and an Access Policy in place? Give details of how the information will be held/ levels of access	☐ Yes ☐ No Please Specify -
Have the information risks been assessed for the system, please provide copies of risk assessments?	☐ Yes ☐ No Please Specify -
Where would the information stored (i.e. Cloud internal etc.)	
Are there contingency plans / backup policies in place to manage the effect of an unforeseen event?	☐ Yes ☐ No
Are there procedures in place to recover data (both electronic and paper) which may be damaged through : • Human error • Computer Virus • Network Failure • Theft • Fire • Flood • Other disaster	☐ Yes ☐ No Please Specify -

Sign off

Data Protection Impact Assessment completed by :

Name	
Job Title	
Name of organisation	
Signature	
Date	

Reviewed and signed by: (DPIA can be reviewed by Senior Partners or Practice Managers)

Name	
Job Title	
Name of organisation	
Signature	
Date	
Comments if applicable	

Reviewed and Approved by:

Name	
Job Title	Data Protection Officer (DPO)
Name of organisation	
Signature	
Date	
Comments if applicable	

Appendix A – Generic Duties of Information Asset Owner and Information Asset Administrators (System Managers)

System Management Duties

The duties of a system manager / Information Asset Owner will vary considerably with each system, but will usually consist of the following

General System Management

- Be the lead contact person for the system.
- Thoroughly understand the system and how best it can benefit the department.
- Take ownership of the system and manage it day to day
- Assist in and advise on change management
- Advise on system development, enhancements etc.
- Attend system user groups as appropriate.
- Where appropriate, respond to Subject Access Requests for information pertaining to a patient or member of staff.

Data Quality

- Take ownership of the data held within the system, ensuring it is accurate, kept up to date and in keeping with Data Protection and Caldicott standards.
- Undertake Data Quality and validation audits, design and implement improvement plans

User Support

- Be the first line support i.e., contact IT or the supplier as appropriate.
- Provide training as appropriate.

Security Issues

- Ensure the system is operated in compliance with the Practice's Information Governance policy and its standards and procedures.
- Ensure risks are reported to the IG Lead on a quarterly basis.
- Administer the systems access, issuing and removing passwords as appropriate.
- Ensure the systems security and complete a detailed 'System Level Security Policy' (SLSP) including a risk assessment.
- Help develop contingency arrangements for system failure.