Data Protection Impact (DPIA) Assessment Policy

JENNER HOUSE SURGERY

Published:	March 2019
Review Date:	March 2021
Approval signature:	APPROVED
Version:	Version 1 (New)
Acknowledgements	

Introduction

This policy reinforces the principles of Information Governance and Data Protection. The document outlines the Practice's approach and methodology for Data Protection Impact Assessments for new and existing systems and processes.

It is important that all new processes, policies, projects, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

The policy details the process to be followed to ensure a formal assessment is completed to determine whether any proposed changes to the Practice's processes, policies, projects and/or information assets impacts on the integrity and accessibility of personal information.

Some of the considerations that should be taken into account are whether a new process, project or information asset will:

- Affect the quality of personal information already collected;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required or in accordance with The Records Management: NHS Code of Practice;
- Have an adequate level of technical and organisational security measures to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
- Enable data retrieval to support business continuity in the event of an emergency;
- Enable the timely location and retrieval of personal information to meet a subject access request; and
- Alter the way in which the Practice captures information within / monitors information from a key system.

The rationale for conducting a DPIA is to:

- Identify and manage risk;
- Avoid unnecessary costs and inadequate solutions;
- Avoid loss of trust and reputation;
- Inform the Practice's communications strategy; and
- Meet legal requirements in terms of information security, data protection and confidentiality.

The policy applies to information held in both manual and electronic form.

This policy applies to all staff who work for the Practice including contractors, who are responsible for project managing a new project, implementation of a new process or plan to modify a current system (information asset).

Data Protection Impact Assessment (DPIA) Process

A DPIA must be carried out in addition to compliance checking or a data protection audit, and conducted at a stage when the outcome can genuinely affect the development of a project or process.

An effective DPIA will help identify and avoid problems which may not be obvious at the conception stage and should form an intrinsic part of the overall risk assessment.

When should a DPIA be undertaken?

Not every new project, system or change in process will require a DPIA. The Information Commissioner's Office (ICO) recommends that DPIAs are completed to comply with a change in law, introduction of new or intrusive technology or where person identifiable or sensitive information which was originally collected for a limited purpose is going to be collected for any new purpose(s) or reused in a new and unexpected way.

Completion of the initial DPIA Screening Questionnaire (Appendix 1) will ensure that a full DPIA is completed only when necessary and provide evidence to support the Practice's Information Governance agenda.

Best practice dictates that the initial screening questionnaire should be started when:

- The project / process is being designed and the scope has been agreed;
- Before a system has been procured;
- Before contracts/MOUs/agreements have been signed.
- For all QIPP projects as a mandatory assessment within each Project Initiation Document (PID)

Who Is Required to Complete a DPIA?

The DPIA template, which includes initial screening questions will be completed by the Primary Care Data Protection Officer in conjunction with the project manager or individual responsible for overseeing the project from the provider wishing to execute the project within the Practice. The Data Protection Officer for our area has confirmed that the Practice should not complete the DPIA (9th January 2019). The rationale for this is the team best placed to list the technologies and intricacies of the project or programme; is the provider themselves.

The DPIA will then be passed to the DPO for assessment. The DPO will then seek approval from the Commissioning Support Unit Information Governance Team, who will then advise the Practice on sign up.

Applying the Outcome of the Initial Screening Questionnaire

Where answers to questions are 'Yes', a full scale DPIA should be completed with support from the Data Protection Officer.

Definitions

Data Protection Impact Assessment	A risk technique mandated by the General Data Protection Regulations to enable organisations to address privacy concerns and ensure appropriate technical and organisational safeguards are addressed and built in to new projects / processes / policies / amendments of existing systems
Projects / processes / policies / amendments of existing systems	DPIAs are required when new projects occur (e.g. introduction of a new electronic patient record, process involving the transfer and/or use of information between providers of a service) or where plans are proposed to develop an existing information asset. These can be both paper and electronic.
Special Category data	Under the Data Protection Act this is data such as patient diagnosis, medical history, ethnicity, sex, religion.
Personal data	Data which is capable of identifying an individual, but isn't classified as special category data, for example, name, postcode, GP, next of kin, address, date of birth and so on.
Privacy-invasive technology	Privacy-invasive software is a category of computer software that ignores users' privacy and that is distributed with a specific intent, often of a commercial nature/mass marketing, which negatively affects its users. Examples include, but are not limited to, locator technologies such as global positioning systems (GPS) and mobile phone locators, biometric scanners.

Roles and Responsibilities

The Governing Body (CSU)

The Governing Body owns the information governance strategy & framework and the implementation of measures to minimise information risk and safeguard the interests of its staff, patients and information assets of the Practice.

Senior Information Risk Owner (SIRO)

The SIRO is responsible to the Governing Body for ensuring an Information Governance strategy & framework is implemented, reviewed and its effect monitored. Privacy Impact Assessment is one element of the management of IG and information risk.

The SIRO will:

- Take ownership of the Practice's information risks;
- Act as the advocate for information risk on the Governing Body;
- Provide written advice to the Chief Officer, as detailed in the Annual Governance Statement; and
- Occupy a key role in ensuring effective management and identification of information risks.
- Oversees all QIPP projects and ensure they have a completed PIA

Information Asset Owners

An Information Asset Owner has responsibility for managing aspects of the Practice's business, and therefore will be responsible for knowing what information assets are held by their team, understanding the potential risks to the assets and to provide assurance to the Practice's SIRO concerning the security, confidentiality, integrity and use of the assets. Their roles include:

- Understanding what information is held;
- Knowing what is to be added and removed;
- Knowing how information is moved / transferred;
- Knowing who has access and why; and
- Ensuring compliance with the relevant legal frameworks, i.e. consent and confidentiality

Information Asset Administrators

As an Information Asset Administrator, with day-to-day responsibility for the creation, receipt, use and storage of information assets, IAAs will provide support to the Information Asset Owner for their team to ensure that:

- The Information Asset Register is kept up to date
- Policies and procedures regarding information management and risk are followed
- Actual or potential information risks are recognised and reported; and
- Information sharing agreements are complied with.

Data Protection Office (DPO)

The DPO is responsible for assessing and manage the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. This will be achieved by reviewing the outcome of the DPIA to ensure compliance with the GDPR and national data protection legislation is maintained.

Monitoring and Review

The SIRO, will receive regular reviews of information and will review all PIAs as part of Project Initiation.

The Practice Manager will formally monitor the implementation and performance of this document by:

- reviewing progress against the IG Toolkit/DSP Toolkit;
- considering IG risk mitigation plans;
- ensuring a programme of internal/external audit reviews (including audit of the IG Toolkit/DSP Toolkit self-assessment); and
- monitoring the implementation of audit recommendations.

This policy will be reviewed every 2 years by the Practice Manager, or sooner should changes in legislation or guidance require it.

APPENDIX A – DPIA TEMPLATE

NHS
South, Central and West
Commissioning Support Unit

Project:	
Document Title:	
Author:	
Version	
Status:	

Version History

Revision Date	Version Number	Summary of Changes	Changes Marked

Reviewed by
This document (or its component) parts have been reviewed by the following

Name	Title & Company	Issue Date	Version

Approvals
This document requires the following approvals:

Name	Signature	Title	Date of Issue

Distribution
This document has been distributed to :

Name	Title & Company	Date

Contents

1. Introduction

A Data Protection Impact Assessment (DPIA), (formerly known as privacy impact assessment or PIA), is a method of helping organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.
You must carry out a DPIA when:

- using new technologies; and the processing is likely to result in a high risk to the rights and freedoms of individuals

- Processing that is likely to result in a high risk includes (but is not limited to): systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals

- large scale processing of special categories of data or personal data relation to criminal convictions or offences; this includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity large scale, systematic monitoring of public areas (CCTV)

2. Data Protection Impact Assessment Process

- All new proposals for processing of data are required to undertake the screening process (see below) to establish whether a full DPIA is needed

- Completing the screening process and the DPIA are the responsibility of the Project Manager or Sponsor

- The DPIA must be reviewed and signed by an appropriate authorising officer (Data Protection Officer/Senior Information Risk Owner/Caldicott Guardian)

- Where appropriate, information risk should be recorded in existing documentation, e.g. project risk register, corporate risk register

- The DPIA must be updated if changes to the processing are proposed and reviewed at appropriate stages

- Remember to record all information assets and data flows on your Information Asset Register and Data Flow Map

3. Screening Questions

Project ID:	**Date:**		
Project Manager:			
DPIA Screening Questions	**Yes (x)**	**No (x)**	**Comments**
Will the project involve the collection of new information about individuals?			
Will the project compel individuals to provide information about themselves?			
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?			
Do you propose using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?			
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.			
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?			
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. health records, criminal records or other information that people would consider to be particularly private.			
Will the project require you to contact individuals in ways which they may find intrusive?			
Will the project store information using cloud technology?			
Will the project transfer information outside the European Economic Area?			

- If you answered **no** to all the questions, you **DO NOT** need to proceed to a full Data Protection Impact Assessment. Save this document to evidence your assessment

- If you answer **yes** to any of these questions, you **DO** need to proceed to a full Data Protection Impact Assessment. Complete the following sections and save to evidence your assessment

4. Full DPIA

Steps	Requirements	Suggested Accompanying Documents
1. Identify the need for a DPIA	• Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.	
2. Describe the information flows	• Describe the collection, use and deletion of personal data • Identify individuals who are likely to be affected by the project	
Note: Discuss the project with your IG Lead/Data Protection Officer		
3. Identify the privacy and related risks	• Identify the key privacy risks and the associated compliance and corporate risks. • Activities may include discussions and workshops with stakeholders and the IG Lead • Data Protection Principles found below should be used to help identify the Data Protection Legislation related compliance risks.	
Identify privacy solutions	• Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).	

Steps	Requirements	Suggested Accompanying Documents
Agree and record the DPIA outcomes	• Agree risk owners and action owners • Apply mitigation and reassess risk • Record recommendations here	
Integrate the DPIA outcomes back into the project plan	• Identify who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork • Identify who is responsible for implementing the solutions that have been approved • Identify who the contact is for any privacy concerns which may arise in the future	
Signoff by authorised officer: **Name:** **Role:** **Signature:** **Date:**		

5. Linking the DPIA to Data Protection Legislation.

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the Data Protection Legislation and other relevant legislation, for example the Human Rights Act and the Common Law Duty of Confidentiality.

Principle 1 (a), from the GDPR Article 5 - Lawfulness, fairness and transparency

Previous DPA98 Principle 1 - Personal data shall be processed fairly and lawfully

- Have you identified the purpose of the project?
- What is the legal basis for processing?
- How will individuals be told about the use of their personal data?
- Do you need to amend your privacy notices?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

If your organisation is subject to the Common Law Duty of Confidentiality, you also need to consider:

- Will the information be given under a Duty of Confidentiality?

Principle 1 (b) from the GDPR Article 5 - Purpose limitation

Previous DPA98 Principle 2 - obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?

Principle 1 (c) from the GDPR Article 5 – Data minimisation

Previous DPA98 Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the information you are using of good enough quality for the purposes it is used for?
- Which personal data could you not use, without compromising the needs of the project?

Principle 1 (d) from the GDPR Article 5 - Accuracy

Previous DPA98 Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- How will you maintain accuracy over time?

Principle 1 (e) from the GDPR Article 5 - Storage Limitation

Previous DPA98 Principle 5 - not be kept for longer than necessary for that purpose or those purposes.

- What retention periods are applicable for the personal data you will be processing?

- Are you procuring software which will allow you to delete information in line with your retention periods?
- Could you set the software to automatically delete information on its disposal date?

From the GDPR Articles 12 – 23 - Individual rights

Previous DPA98 Principle 6 - processed in accordance with the rights of data subjects

- Do you need consent of the individual to process this information?
- How can you take account of objections to the processing?
- Will the systems you are putting in place allow you to respond to subject access requests more easily?
- Are you processing information of children aged 13-16?
- If the project involves marketing, have you got a process for individuals to opt **IN** to their information being used for that purpose?
- How do you consider and action requests to cease processing?
- How do you consider and action requests to delete an individual's information?

Principle 1 (f) from the GDPR Article 5 – Integrity and Confidentiality

Previous DPA98 Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data.

- Do the new systems provide adequate protection against the security risks you have identified?
- What training and instructions are necessary to ensure that all staff know how to operate a new system securely?
- If you are transferring data, how will this be done securely?
- How will you protect the data at rest?

From the GDPR Article 3 – Territorial Scope

Previous DPA98 Principle 8 - not transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?