Sherwood Forest Hospitals
NHS Foundation Trust

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

Document Category:	**INFORMATION GOVERNANCE**
Document Type:	**PROCEDURE**

Keywords:	Privacy Impact Assessment, Data Protection Act 2018 2018 UK GDPR

Version:	**Issue Date:**	**Review Date:**
4	April 2023	April 2025

Supersedes:	Version 3		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	4th April 2023

Scope/ Target Audience: (delete as applicable / describe)	All staff and patients
Evidence Base/ References:	See Section 10
Lead Division:	Corporate
Lead Specialty:	Information Governance
Lead Author:	Information Governance Manager and Data Protection Officer
Sponsor:	Director of Corporate Affairs

	Name the documents here or record not applicable
Associated Policy	Data Protection Impact Assessment Policy, Data Protection, Confidentiality and Disclosure Policy
Associated Guideline(s)	
Associated Pathway(s)	
Associated Standard Operating Procedure(s)	
Other associated documents e.g. documentation/ forms	

Consultation Undertaken:	Information Governance Committee Information Governance Working Group
Template control:	v1.4 November 2019

CONTENTS

1 INTRODUCTION/ BACKGROUND

A Data Protection Impact Assessment (DPIA) is a process designed to help organisations analyse, identify and minimise the Data Protection risks[1] of a project or plan. It is a key part of our accountability obligations under UK General Data Protection Regulation, and when done properly helps the Trust assess and demonstrate how we comply with all of our Data Protection obligations.

It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

2 AIMS/ OBJECTIVES/ PURPOSE (including Related Trust Documents)

An effective Data Protection Impact Assessment (DPIA) allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and the Trust.

Conducting and publishing a Data Protection Impact Assessment (DPIA) will help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations.

A Data Protection Impact Assessment (DPIA) can cover a single processing operation, or a group of similar processing operations. You may even be able to rely on an existing Data Protection Impact Assessment (DPIA) if it covered a similar processing operation with similar risks. A group of organisations can also do a joint Data Protection Impact Assessment (DPIA) for a group project or industry-wide initiative.

For new technologies, you may be able to use a Data Protection Impact Assessment (DPIA) done by the product developer to inform your own Data Protection Impact Assessment (DPIA) on your implementation plans.

For new projects, Data Protection Impact Assessments (DPIA) is a vital part of Data Protection by design. They build in Data Protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented. No commitments to, or installation of systems, should take place before the DPIA has been signed off.

[1] Risk in this context is about the potential for any significant physical, material or non-material harm to individuals

You should not view a Data Protection Impact Assessment (DPIA) as a one-off exercise to file away. A Data Protection Impact Assessment (DPIA) is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an on-going basis. You need to keep it under review and reassess if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your Data Protection Impact Assessment (DPIA) assesses any new risks.

Related Trust Documents

- Data Protection, Confidentiality and Disclosure Policy
- Data Protection Impact Assessment Policy
- Information Security Policy
- Network Security Policy

3 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer

We are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Caldicott Guardian and works with the Senior Information Risk Owner and the Caldicott Guardian.

The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data

Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Information Asset Owners (IAOs)

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)

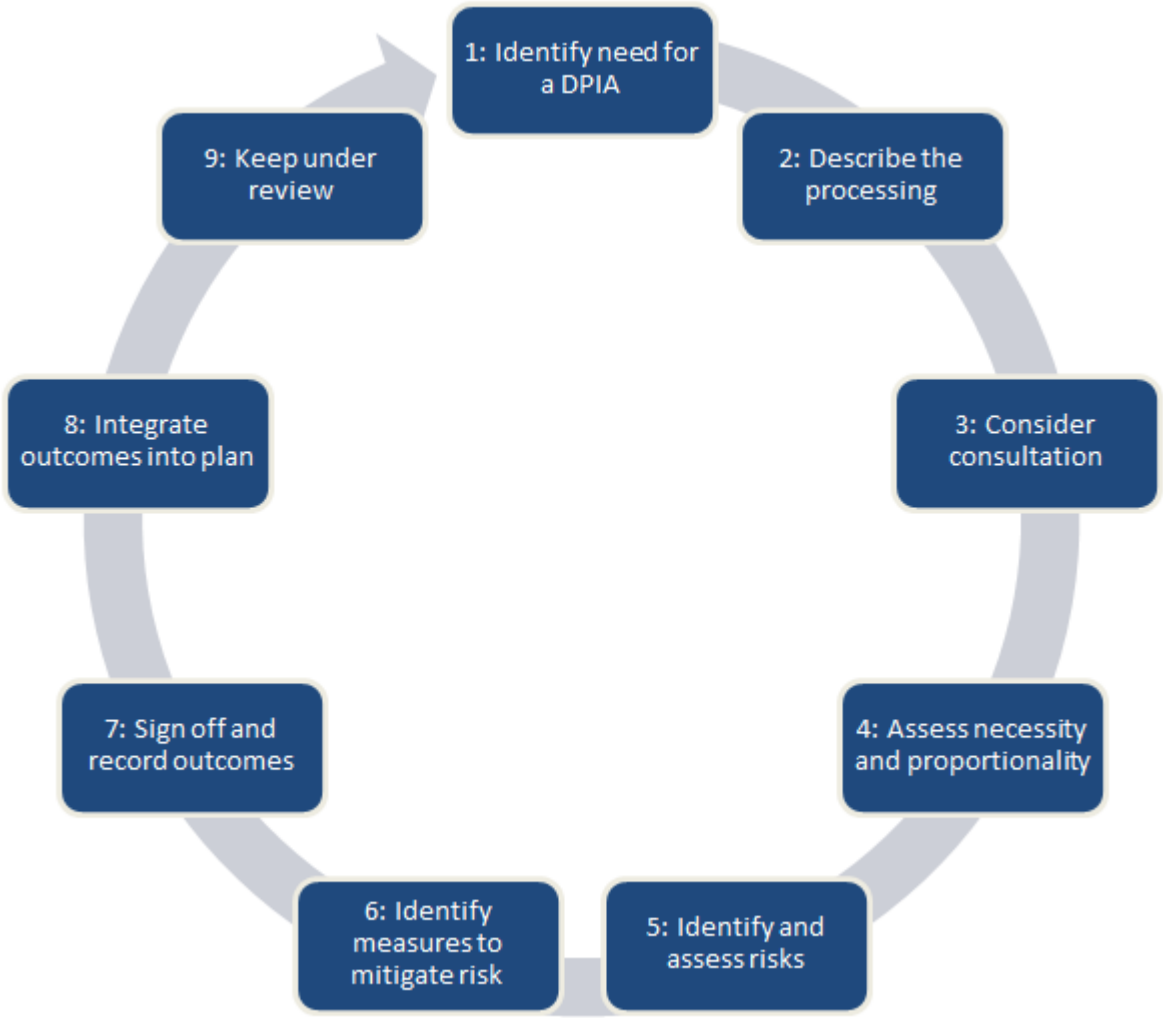
Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

All Staff

All Trust employees (including Medirest and Skanska colleagues) and anyone else working for The Trust (e.g. agency staff, honorary staff, management consultants etc.) who use and have access to Trust personal information must understand their responsibilities for Data Protection and confidentiality.

4 HOW DO I UNDERTAKE A DATA PROTECTION IMPACT ASSESSMENT?

The diagram below details the various stages of a Data Protection Impact Assessment.



4.1 WHO SHOULD CARRY OUT A DATA PROTECTION IMPACT ASSESSMENT

The Trust is responsible for ensuring that the Data Protection Impact Assessment (DPIA) is carried out. Data Protection Impact Assessments (DPIA) may be done by someone else, inside or outside the organisation, but the Trust remains ultimately accountable. Data Protection Impact Assessments should be completed by Information Asset Owners/Administrators who have good knowledge of the project, the systems involved and the level of information required. It is likely that multiple staff from the project and suppliers (if one is used) will need to be involved with carrying out the Data Protection Impact Assessment.

The Trust must also seek the advice of the Data Protection Officer (DPO), and this advice, and the decisions taken by the Trust, should be documented within the Data Protection Impact Assessment (DPIA). The Data Protection Officer should also monitor the performance of the Data Protection Impact Assessment (DPIA).

If the project is wholly or partly performed by a third party (data processor), **the third party should assist the Trust in carrying out the Data Protection Impact Assessment (DPIA)** and provide any necessary information.

The Trust must also **"seek the views of data subjects (individuals) or their representatives", where appropriate"**. The Trust should also document its reasoning for not seeking the views of individuals, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.

4.2 IDENTIFY NEED FOR A DATA PROTECTION IMPACT ASSESSMENT

In most cases, a combination of two of these factors (below) indicates the need for a Data Protection Impact Assessment (DPIA) and you will need to complete the DPIA template. However, in some cases, the Trust can consider that processing meeting only one of these criteria requires a Data Protection Impact Assessment, therefore you will need to complete the template.

Conducting a Data Protection Impact Assessment (DPIA) is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a **high risk[2] to the rights and freedoms of individuals.**

In order to provide a more concrete set of processing operations that require a Data Protection Impact Assessment (DPIA), the following eleven criteria should be considered. **In most cases, a combination of two of the eleven factors indicates the need for a Data Protection Impact Assessment (DPIA). However, in some cases, the Trust can consider meeting only one of the eleven factors.** The Data Protection Impact Assessment Policy is available on the Trust's website where there are screening questions which will help you decide whether a Data Protection Impact Assessment is required.

1. **Evaluation or scoring** - including profiling, predicting and transactional monitoring techniques. For example, a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks; a new system that might be susceptible to fraud or abuse, and if so whether it ensures that the system has the capability for transactional level monitoring so you can audit the transactions if needed as part of an investigation.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

2. **Automated decision making with legal or similar significant effect** - processing that aims at taking decisions on individuals. For example, the processing may lead to the exclusion or discrimination against individuals.

3. **Systematic monitoring of individuals** - processing used to observe, monitor or control individuals. For example, CCTV, monitoring of the employees' work station, internet activity, etc.

4. **Sensitive data or data of a highly personal nature** - this includes special categories of personal data (for example information about individuals' health care, racial or ethnic origin etc.).

5. **Data processed on a large scale** – how many individuals concerned, either as:
   a. a specific number or as a proportion of the relevant population;
   b. the volume of data and/or the range of different data items being processed;
   c. the duration, or permanence, of the data processing activity;
   d. the geographical extent of the processing activity.

6. **Matching or combining datasets** - for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject

7. **Data concerning vulnerable individuals** - individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable individuals may include children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.).

8. **Innovative use or applying new technological or organisational solutions** - combining the use of finger print and face recognition for improved physical access control.

9. **Preventing individuals from exercising a right or using a service or contract** - When the processing in itself "prevents individuals from using a service or a contract". An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

10. **Offer online services directly to children -** Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved. If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.

11. **Storing or transmitting data outside the EU/EEA -** You may make a restricted transfer if the receiver is located in a third country or territory, or is an international organisation, or in a particular sector in a country or territory, covered by UK 'adequacy regulations'. You can make a restricted transfer if it is covered by a legal instrument between public authorities or bodies containing 'appropriate safeguards'.

The appropriate safeguards must include enforceable rights and effective remedies for people whose personal data is transferred.

12. **Direct marketing e.g. newsletters, email subscriptions -** Direct marketing can add value to the customer experience. It can make people aware of new products and services that they may benefit from, give them opportunities to take part in events, or find out about important causes. When done responsibly direct marketing can also increase trust and confidence in your brand or organisation. However, direct marketing has the potential to cause nuisance to people, and in some cases it can cause them harm and distress.

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

Examples of processing	**Possible Relevant criteria**	**DPIA likely to be required?**
A hospital processing its patients' genetic and health data (hospital information system).	✓ Sensitive data or data of a highly personal nature. ✓ Data concerning vulnerable data subjects. ✓ Data processed on a large-scale.	Yes
A data sharing initiative between organisations to pool or link sets of personal data.	✓ Sensitive data or data of a highly personal nature. ✓ Data concerning vulnerable data subjects. ✓ Data processed on a large-scale.	
A new database/system that consolidates information held by separate parts of an organisation	✓ Sensitive data or data of a highly personal nature. ✓ Data concerning vulnerable data subjects. ✓ Data processed on a large-scale.	
The use of a camera system to monitor driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates	✓ Systematic monitoring. ✓ Innovative use or applying technological or organisational solutions.	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	✓ Systematic monitoring. ✓ Data concerning vulnerable data subjects	
The gathering of public social media data for generating profiles.	✓ Evaluation or scoring. ✓ Data processed on a large scale. ✓ Matching or combining of datasets. ✓ Sensitive data or data of a highly personal nature	
An institution creating a national level credit rating or fraud database.	✓ Evaluation or scoring. ✓ Automated decision making with legal or similar significant effect.	

	✓ Prevents data subject from exercising a right or using a service or a contract. ✓ Sensitive data or data of a highly personal nature	
Storage for archiving purpose of pseudonymised confidential patient information concerning vulnerable data subjects of research projects or clinical trials	✓ Sensitive data. ✓ Data concerning vulnerable data subjects. ✓ Prevents data subjects from exercising a right or using a service or a contract.	

4.3 HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT

- Complete the screening questions[3] and send to the Information Governance team for review sfh-tr.information.governance@nhs.net. The Information Governance team will let you know the outcome of the screening questions.
- If after conducting a Data Protection Impact Assessment screening process, it appears that a Data Protection Impact Assessment is not required then the Data Protection Impact Assessment screening form will need to be completed and signed by the Information Asset Owner and Information Governance Lead.
- If the Information Governance team advise that a Data Protection Impact Assessment is required the DPIA template to be completed is available here[4]. The following guidance in steps 4.3 to 4.6 will assist you in completing the template. Once completed you will need to send to the Information Governance team for review sfh-tr.information.governance@nhs.net.

4.4 SIGN OFF

The Information Governance team will discuss the project at the Information Governance working group and the Information Asset Owner and/or administrator will be asked to attend and answer any questions by members. Once reviewed and any changes are made, the Data Protection Impact Assessment will be sent by the Information Governance team in the following order for individual approval:

1. Data Protection Officer
2. Information Commissioner's Office (if required)
3. Information Asset Owner
4. Caldicott Guardian and Senior Information Risk Owner.

4.5 INTEGRATE OUTCOMES INTO PLAN

Any outstanding risks and/or recommendations will need to be integrated into the project plan.

4.6 KEEP UNDER REVIEW

It is important to note that the Data Protection Impact Assessment is a 'live' document and should be considered as part of a management lifecycle for the project. Data Protection Impact Assessments will be published on the website here[5].

[3] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8644
[4] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8644
[5] https://www.sfh-tr.nhs.uk/about-us/information-governance/data-protection-impact-assessments/

5 EDUCATION AND TRAINING

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include UK General Data Protection Regulations (UK GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation
A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.

6 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Audit of completed Data Protection Impact Assessments (DPIAs)	Information Governance Team	Audit	Annually	Information Governance Committee
Adherence to Information Governance policies and procedures in nominated Division/ Department	360 Assurance	Audit	Annually	Information Governance Committee

7 EQUALITY IMPACT ASSESSMENT (please complete all sections)

Name of service/policy/procedure being reviewed: Data Protection Impact Assessment Procedure			
New or existing service/policy/procedure: Existing			
Date of Assessment: 9th February 2023			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?	b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?	c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality
The area of policy or its implementation being assessed:			
Race and Ethnicity:	None	Not applicable	None
Gender:	None	Not applicable	None
Age:	None	Not applicable	None
Religion:	None	Not applicable	None
Disability:	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality:	None	Not applicable	None
Pregnancy and Maternity:	None	Not applicable	None
Gender Reassignment:	None	Not applicable	None
Marriage and Civil Partnership:	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation):	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out? • None
What data or information did you use in support of this EqIA? • Trust guidance for completion of the Equality Impact Assessments
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? • No

Level of impact From the information provided above and following EqIA guidance document please indicate the perceived level of impact: Low Level of Impact

Name of Responsible Person undertaking this assessment: Gina Robinson
Signature: Gina Robinson
Date: 9th February 2023

8 APPENDICES

Appendix A - Data Protection Impact Assessment Policy
Appendix B - Screening questions
Appendix C - Data Protection Impact Assessment Template