Tees, Esk and Wear Valleys
NHS Foundation Trust

# Data Protection Impact Assessment (DPIA) Procedure

# Ref IT-0030-001-v1

**Status: Approved**
**Document type: Procedure**
**Overarching Policy: Data Management Policy**

## Contents

**1 Introduction....3**
**2 Purpose....3**
**3 Scope....3**
3.1 What this procedure applies to....3
3.2 Who this procedure applies to....4
**4 Related documents....4**
**5 Process....5**
5.1 Identify the need for a DPIA....5
5.2 Has the system ever had a DPIA?....5
5.3 Where do I obtain a DPIA form?....5
5.4 Completing the DPIA form(s)....5
5.5 Anonymised/pseudonymised data....5
5.6 Publication....6
5.7 DPIA process flow....7
**6 Roles and responsibilities....8**
**7 Definitions....9**
**8 How this procedure will be implemented....9**
8.1 Training needs analysis....9
**9 How the implementation of this procedure will be monitored....9**
**10 Document control....10**

# 1 Introduction

Data Protection Impact Assessment (DPIA) is a process for identifying and minimising the data protection risks of a project or change.

A DPIA must be carried out whenever there is a change that is likely to involve a new use of personal data, change of process or significantly change the way in which personal data is handled.

Examples include:

- Redesign of an existing process or service;
- Introduction of a new process or information asset.

Data Protection Impact Assessment is mandated by the Data Protection Act 2018 (GDPR). Failure to undertake a DPIA and introducing risk to the rights and freedoms of individuals may result in a fine equivalent to up to 4% of annual turnover.

# 2 Purpose

For all projects, service and system developments, procedures and policies that involve the processing/sharing of personal information, following this procedure will ensure the Trust:-

- Meets its legal obligations in carrying out an assessment of the impact of the envisaged processing operations on the protection of personal data;
- Addresses any privacy concerns and risks raised;
- Ensures the rights and freedoms of individuals are not compromised;
- Comply with the requirement of ‘data protection by design and default’.

# 3 Scope

## 3.1 What this procedure applies to

This procedure is to be followed when:

- Introducing a new paper or electronic information system to collect and hold personal data;
- Updating or revising a key system that might alter the way in which the organisation uses, monitors and reports personal information;
- Changing an existing system where additional personal data will be collected;

- Proposing to collect personal data from a new source or for a new activity;
- Planning to outsource business processes involving storing and processing personal data;
- Planning to transfer services from one provider to another that include the transfer of information assets;
- Changing existing or introducing new data sharing agreements.

This procedure covers all aspects of information, in both paper and electronic format.

## 3.2 Who this procedure applies to

This procedure applies to all permanent, temporary and contracted staff.

The principles of this procedure apply to all third parties and others authorised to undertake work on behalf of the Trust.

# 4 Related documents

This procedure describes what you need to do to implement the Data Protection Act 2018 (GDPR) section of the Data Management Policy to ensure Privacy by Design and Default.

This procedure also refers to:-

- ✓ Maintenance of IT Systems Policy
- ✓ Introduction or Upgrade of Information Systems Procedure
- ✓ Project and Programme Management Frameworks

# 5 Process

## 5.1 Identify the need for a DPIA

Does the process you are planning to introduce or change involve the processing of personal and/or sensitive data?

If you answer 'Yes' to this question, a DPIA is needed.

If you are not sure whether you need a DPIA, contact the Information Department's Compliance Team for advice at tewv.informationsecurity@nhs.net

Each proposed change must be considered on its own merits. If you have made a similar change that did not require a DPIA, do not assume that you will not need one this time.

## 5.2 Has the system ever had a DPIA?

If an existing system has never undergone a DPIA, it is difficult, if not impossible, to determine whether subsequent changes will have any negative impacts.

Existing systems that have never been assessed should have a DPIA carried out before any changes are proposed. This will act as a benchmark from which subsequent changes can be assessed.

## 5.3 Where do I obtain a DPIA form?

If you are managing a project or programme using the Trust's project/programme management framework, the DPIA form is included as part of this framework.

For all other changes, the DPIA form can be obtained from the Information Security Officer or Incident Investigation Officer within the Information Department's Compliance Team via email at tewv.informationsecurity@nhs.net

## 5.4 Completing the DPIA form(s)

The DPIA forms are self-explanatory and include instructions for completion and approval.

## 5.5 Anonymised/pseudonymised data

Any systems which do not identify individuals in any way do not require a DPIA to be performed.

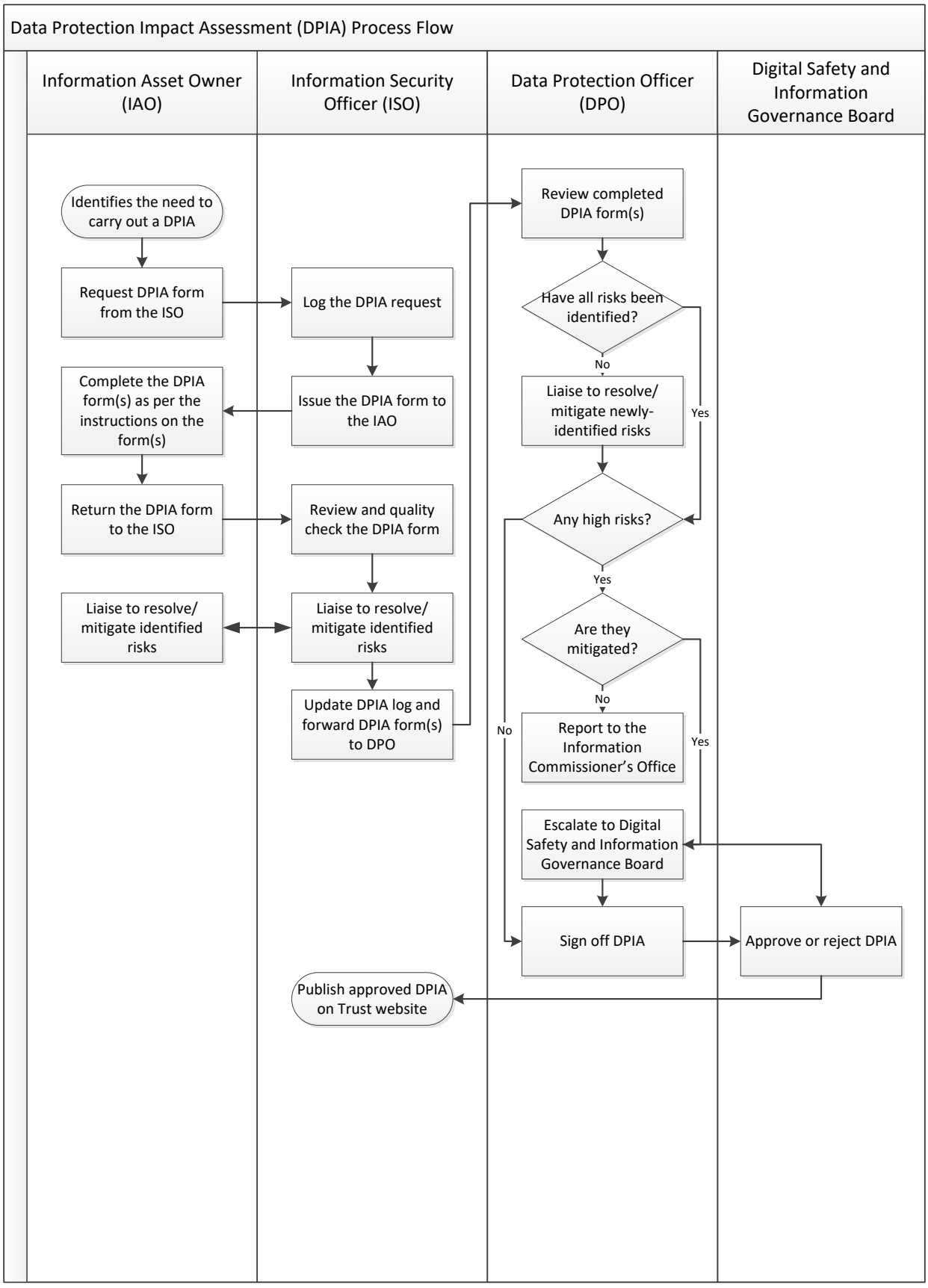
However, it is important to understand that what may appear to be anonymised data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals.

## 5.6 Publication

It is a requirement of the Data Protection Act 2018 (GDPR) that all DPIAs are published to demonstrate transparency of processing.

For the Trust, this is done by the Information Security Officer who publishes approved DPIAs to the external website.

## 5.7 DPIA process flow



# 6 Roles and responsibilities

| Role | Responsibility |
|---|---|
| Chief Executive | • As Accountable Officer, the Chief Executive and the Board of Directors have ultimate accountability for actions and inactions in relation to this document |
| Senior Information Risk Officer (SIRO) | • Overall accountability for Information Governance and Data Security & Protection including privacy and confidentiality.<br>• Briefs the Board of Directors and provides assurance through the Digital Safety and Information Governance Board and the Digital Transformation Board that the Data Security and Protection approach is effective in terms of resource, commitment and execution.<br>• The SIRO for the Trust is the Director of Finance and Information. |
| Caldicott Guardian | • Ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles.<br>• The Caldicott Guardian for the Trust is the Director of Nursing and Governance |
| Data Protection Officer (DPO) | • Ensuring compliance with the Data Protection Act 2018 (GDPR)<br>• Final sign-off of DPIAs before presentation to Digital Safety and Information Governance Board<br>• The DPO for the Trust is the Head of Information Governance |
| Information Security Officer | • Controlling the DPIA process:<br>o Issuing DPIA forms<br>o Keeping a central log of all DPIAs<br>o Receiving and quality checking DPIAs<br>o Working with the Information Asset Owner to ensure all information risks are understood and identified |
| Information Asset Owner (IAO) | • Any person who is responsible for introducing a new or revised service or changes to a new system, process or information asset is the Information Asset Owner (IAO)<br>• Responsible for ensuring the completion and approval of a DPIA before any processing takes place. |
| Digital Safety and Information Governance Board | • Governance group for approval/rejection of DPIAs where mitigated high risk has been identified |
| Technical Change Board | • For the introduction or upgrade of IT systems where |

| | |
|---|---|
| | the use of personal data is involved, TCB is the governance group for ensuring a DPIA has been completed and approved prior to development starting. |

# 7 Definitions

| Term | Definition |
|---|---|
| DPIA | • Data Protection Impact Assessment |
| DPO | • Data Protection Officer |
| IAA | • Information Asset Administrator |
| IAO | • Information Asset Owner |
| SIRO | • Senior Information Risk Owner |
| TCB | • Technical Change Board |

# 8 How this procedure will be implemented

- This procedure will be published on the Trust's intranet and external website.
- Line managers will disseminate this procedure to all Trust employees through a line management briefing.

## 8.1 Training needs analysis

No specific training needs have been identified to implement this procedure.

# 9 How the implementation of this procedure will be monitored

| Auditable Standard/Key Performance Indicators | | Frequency/Method/Person Responsible | Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group). |
|---|---|---|---|
| 1 | Log of DPIAs | Monthly | Digital Safety and Information Governance Board |

# 10 Document control

| | | |
|---|---|---|
| Date of approval: | 07 November 2018 | |
| Next review date: | 07 May 2022 | |
| This document replaces: | N/A | |
| Lead: | Name | Title |
| | Louise Eastham | Head of Information Governance |
| Members of working party: | Name | Title |
| | GDPR steering group | |
| This document has been agreed and accepted by: (Director) | Name | Title |
| | Elizabeth Moody | Director of Nursing and Governance |
| This document was approved by: | Name of committee/group | Date |
| | Digital Safety and Information Governance Board | 07 November 2018 |
| An equality analysis was completed on this document on: | 31 October 2018 | |

**Change record**

| Version | Date | Amendment details | Status |
|---|---|---|---|
| 1 | 07 Nov 2018 | New procedure | Approved |
| | Jul 2020 | Review date extended 6 months | |
| | | | |

## Appendix 1 - Equality Analysis Screening Form

**Please note; The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page**

| | | | | | | |
|---|---|---|---|---|---|---|
| Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc. | Information Governance | | | | | |
| Name of responsible person and job title | Louise Eastham – Head of Information Governance | | | | | |
| Name of working party, to include any other individuals, agencies or groups involved in this analysis | GDPR steering group | | | | | |
| Policy (document/service) name | Data Protection Impact Assessment Procedure | | | | | |
| Is the area being assessed a… | Policy/Strategy | | Service/Business plan | | Project | |
| | Procedure/Guidance | | | X | Code of practice | |
| | Other – Please state | | | | | |
| Geographical area covered | Trust-wide | | | | | |
| Aims and objectives | For all projects, service and system developments, procedures and policies that involve the processing/sharing of personal information, following this procedure will ensure the Trust:-<br>• Meets its legal obligations in carrying out an assessment of the impact of the envisaged processing operations on the protection of personal data;<br>• Addresses any privacy concerns and risks raised;<br>• Ensures the rights and freedoms of individuals are not compromised;<br>• Comply with the requirement of 'data protection by design and default'. | | | | | |
| Start date of Equality Analysis Screening | 31 October 2018 | | | | | |
| End date of Equality Analysis Screening | **31 October 2018** | | | | | |

**You must contact the EDHR team if you identify a negative impact. Please ring Sarah Jay on 0191 3336267/3046**

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?

Staff, patients, carers and family

2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?

| | | | | | |
|---|---|---|---|---|---|
| **Race** (including Gypsy and Traveller) | No | **Disability** (includes physical, learning, mental health, sensory and medical disabilities) | No | **Sex** (Men, women and gender neutral etc.) | No |
| **Gender reassignment** (Transgender and gender identity) | No | **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.) | No | **Age** (includes, young people, older people – people of all ages) | No |
| **Religion or Belief** (includes faith groups, atheism and philosophical belief's) | No | **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) | No | **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) | No |

**Yes** – Please describe anticipated negative impact/s

**No** – Please describe any positive impacts/s

The Data Protection Act 2018 (GDPR) introduced new rights for data subjects. Implementing this procedure will provide assurance to people that, when new/updated systems and processes are introduced, impacts on their data and its security have been considered and risks mitigated or managed.

| | | | | |
|---|---|---|---|---|
| **3.** Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.?<br>**If 'No', why not?** | **Yes** | **X** | **No** | |

| | | |
|---|---|---|
| **Sources of Information may include:**<br>• Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc.<br>• Investigation findings<br>• Trust Strategic Direction<br>• Data collection/analysis<br>• National Guidance/Reports | | • Staff grievances<br>• Media<br>• Community Consultation/Consultation Groups<br>• Internal Consultation<br>• Research<br>• Other (Please state below) |

| |
|---|
| 4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Sex, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership |
| **Yes** – Please describe the engagement and involvement that has taken place |
| The procedure has been out to full Trust-wide consultation to all staff. Staff within the Trust comprise all the protected characteristics. |
| **No** – Please describe future plans that you may have to engage and involve people from different groups |
| |

| | | | | | |
|---|---|---|---|---|---|
| 5. As part of this equality analysis have any training needs/service needs been identified? | | | | | |
| **No** | Please describe the identified training needs/service needs below | | | | |
| A training need has been identified for; | | | | | |
| Trust staff | No | Service users | No | Contractors or other outside agencies | No |
| **Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so** | | | | | |
| The completed EA has been signed off by:<br>You the Policy owner/manager:<br>Type name: Louise Eastham | | | | Date:<br>31/10/2018 | |
| Your reporting (line) manager:<br>Type name: Elizabeth Moody | | | | Date:<br>31/10/2018 | |
| If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please call: 0191 3336267/3046 | | | | | |

## Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

| | Title of document being reviewed: | Yes/No/ Unsure | Comments |
|---|---|---|---|
| **1.** | **Title** | | |
| | Is the title clear and unambiguous? | Y | |
| | Is it clear whether the document is a guideline, policy, protocol or standard? | Y | |
| **2.** | **Rationale** | | |
| | Are reasons for development of the document stated? | Y | |
| **3.** | **Development Process** | | |
| | Are people involved in the development identified? | Y | |
| | Has relevant expertise has been sought/used? | Y | |
| | Is there evidence of consultation with stakeholders and users? | Y | |
| | Have any related documents or documents that are impacted by this change been identified and updated? | Y | |
| **4.** | **Content** | | |
| | Is the objective of the document clear? | Y | |
| | Is the target population clear and unambiguous? | Y | |
| | Are the intended outcomes described? | Y | |
| | Are the statements clear and unambiguous? | Y | |
| **5.** | **Evidence Base** | | |
| | Is the type of evidence to support the document identified explicitly? | Y | |
| | Are key references cited? | Y | |
| | Are supporting documents referenced? | Y | |
| **6.** | **Training** | | |
| | Have training needs been considered? | Y | |
| | Are training needs included in the document? | Y | |
| **7.** | **Implementation and monitoring** | | |

| | Title of document being reviewed: | Yes/No/ Unsure | Comments |
|---|---|---|---|
| | Does the document identify how it will be implemented and monitored? | Y | |
| **8.** | **Equality analysis** | | |
| | Has an equality analysis been completed for the document? | Y | |
| | Have Equality and Diversity reviewed and approved the equality analysis? | | |
| **9.** | **Approval** | | |
| | Does the document identify which committee/group will approve it? | Y | |
| Signature: | | | |