journey to change

NHS
Tees, Esk and Wear Valleys
NHS Foundation Trust

Public – To be published on the Trust external website

Data Protection Impact Assessment (DPIA) Procedure

Ref IT-0030-001-v2.1

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

Contents

1 Introduction....3
2 Purpose....3
3 Scope....4
3.1 What this procedure applies to....4
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?....6
5.4 Completing the DPIA form(s)....6
5.5 Anonymised/pseudonymised data....6
5.6 Publication....6
5.7 Information flows....6
5.8 Mitigating and managing risks....6
5.9 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....10
10 Document control....10

Appendix 1 - Equality Analysis Screening Form....12
Appendix 2 – Approval checklist....15
Appendix 3 – Example risks....17

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. 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.

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, the Trust has committed to three goals. This procedure supports all three goals of Our Journey To Change.

Goals 1 (To co-create a great experience for patients, carers and families) and 2 (To co-create a great experience for our colleagues): The Data Protection Act 2018 gives transparency to all aspects of the way that personal information is processed within the Trust. Implementing this procedure provides assurance to patients, careers, families and staff that when systems and processes are introduced or changed, their privacy has been considered from the outset.

Goal 3 (To be a great partner): Information and its governance is a key communication tool and is strategic in assisting the Trust when it works with key partners either to improve services or to jointly care for patients. When we tell our patients who we work with and have robust agreements about what is going to be shared we enable information to support outstanding care and service delivery with our partners.

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’;
- Support the NHSE/I Digital Technology Assessment Criteria (DTAC) as part of the due diligence process.

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 and/or information flows.

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

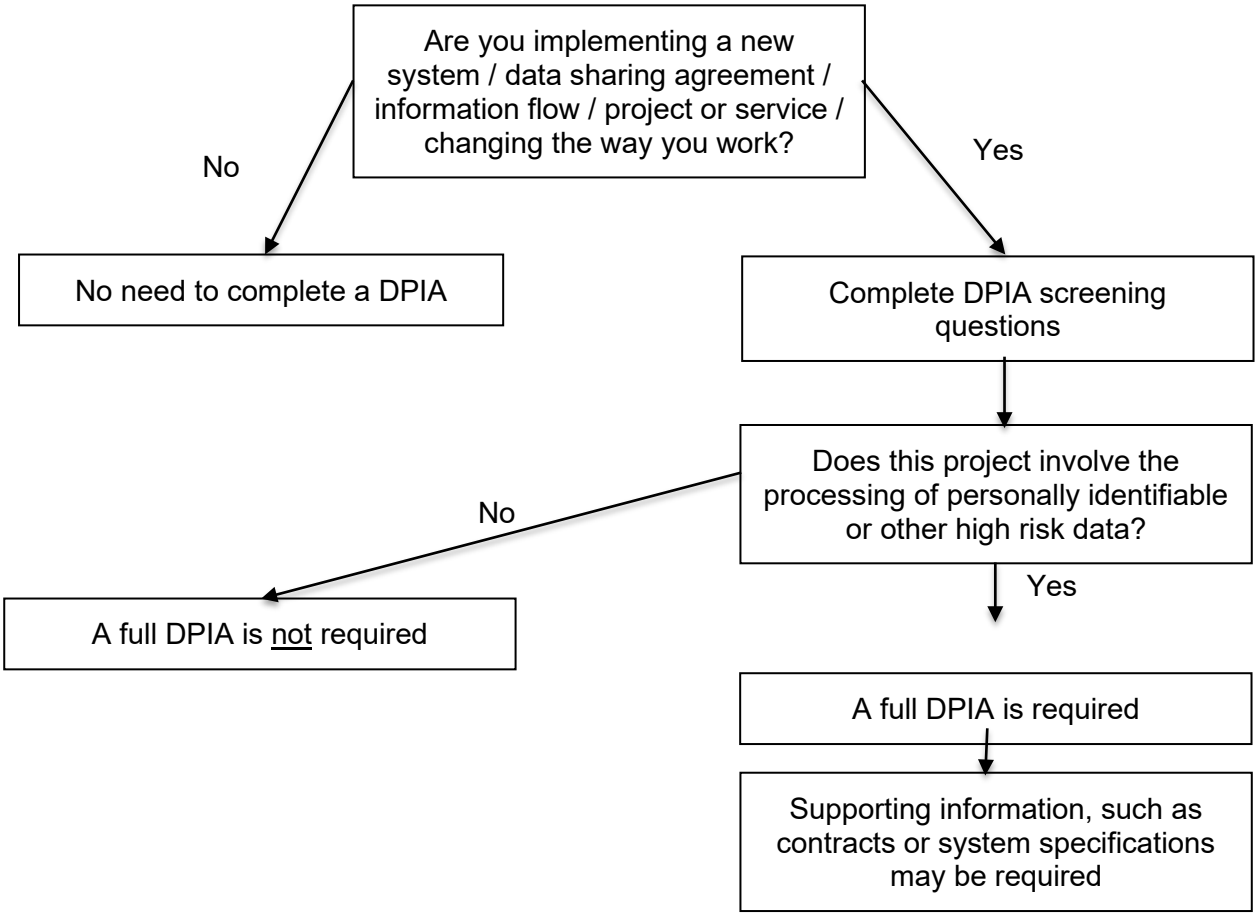
This procedure describes what you need to do to implement the Data Protection Act 2018 section of the Data Management Policy to ensure Privacy by Design and Default.

This procedure also refers to:-

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

5 Process

5.1 Identify the need for a DPIA



If you are not sure whether you need a DPIA, email tewv.dpia@nhs.net for advice.

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 Governance team via tewv.dpia@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 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 Information flows

Information flow mapping is reviewed and updated when there is new or changed processing activity involving personal data. Information flows will be signed off by senior management at least once every twelve months as a requirement of the Data Security and Protection Toolkit.

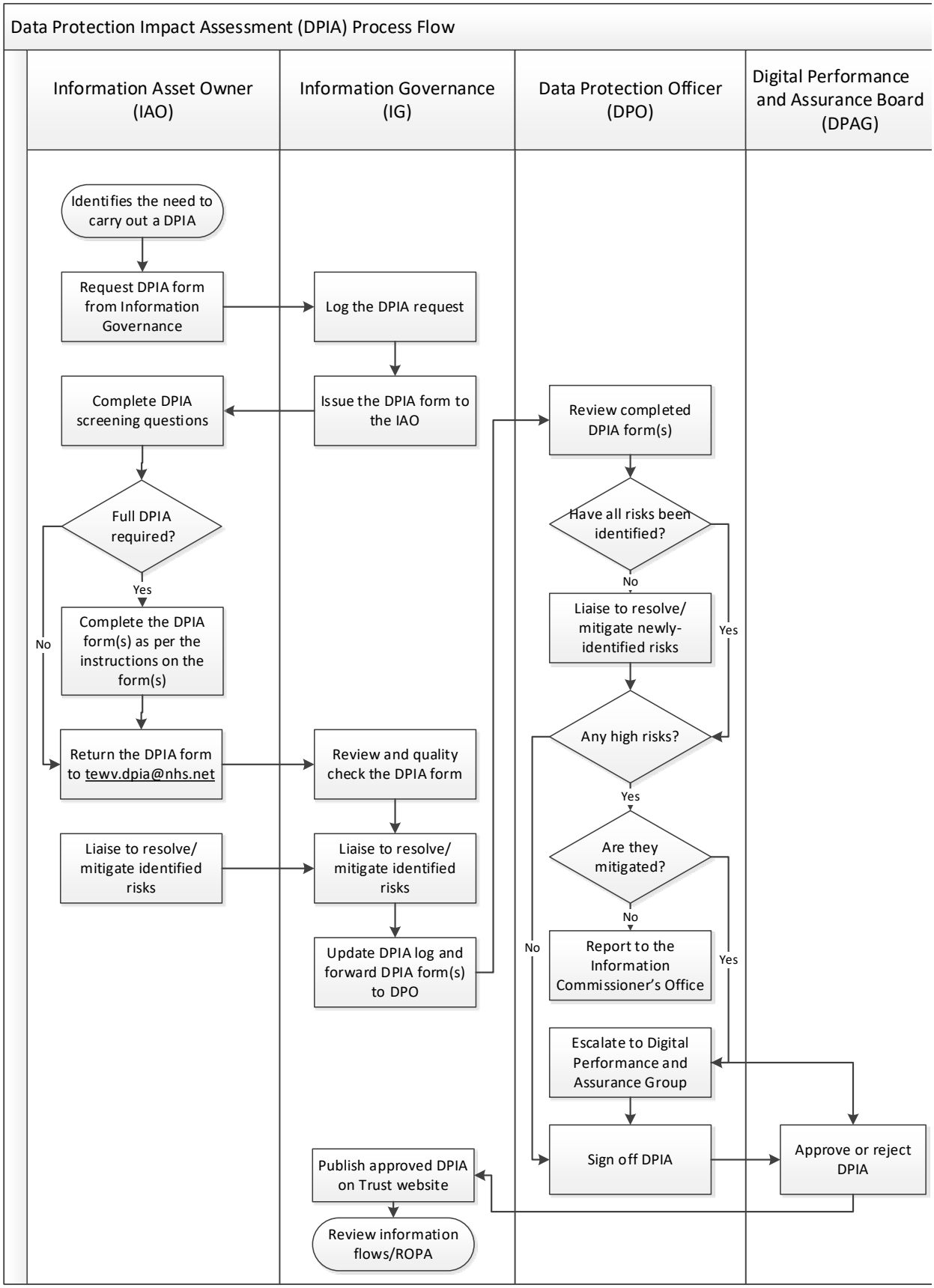
5.8 Mitigating and managing risks

Any high risks must be escalated to the Digital Performance and Assurance Group (DPAG) for final approval or rejection of the DPIA before any processing takes place. Any residual high risks that cannot be mitigated must be reported to the ICO.

Any residual project risks will be recorded and managed via the project's Risks, Assumptions, Issues and Decisions (RAID) log.

Residual risks may have follow-on actions following project closure and require monitoring. Those that remain will be logged on the Trust's risk management system Datix and a risk manager and owner assigned – see Operational Risk Policy for the Trust approach to managing risk.

5.9 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. • Briefs the Board of Directors and provides assurance through the Digital Performance and Assurance Group (DPAG) that the Data Security and Protection approach is effective in terms of resource, commitment and execution. • 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. • 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 • Final sign-off of DPIAs before presentation to DPAG • The DPO for the Trust is the Head of Information Governance

Information Security Officer	• Controlling the DPIA process:
	  ○ Issuing DPIA forms
	  ○ Keeping a central log of all DPIAs
	  ○ Receiving and quality checking DPIAs
	  ○ 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) • Responsible for ensuring the completion and approval of a DPIA before any processing takes place.
Information Risk Management Group	• The governance group with responsibility for monitoring low and medium information risks
Digital Performance and Assurance Group	• Governance group for approval/rejection of DPIAs where mitigated high risk has been identified

Change Assurance Group (CAG)	• For the introduction or upgrade of IT systems where the use of personal data is involved, CAG is the governance group for: ○ ensuring a DPIA has been completed and approved prior to development starting ○ that the DPIA is reviewed through the development lifecycle ○ that the final DPIA reflects the final development prior to its approval and sign-off.

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	Information Governance Group
2	DPIA risk summary	Quarterly	Digital Performance and Assurance Group

10 Document control

Date of approval:	05 April 2022	
Next review date:	31 December 2026	
This document replaces:	IT-0030-001-v2 Data Protection Impact Assessment Procedure	
Lead:	Name	Title
	Andrea Shotton	Head of Information Governance
Members of working party:	Name	Title
This document has been agreed and accepted by: (Director)	Name	Title
	Kam Sidhu Liz Romaniak	Chief Information Officer Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Information Management Meeting Digital Performance and Assurance Group	05 April 2022 **01 June 2022**
An equality analysis was completed on this document on:	29 March 2022	

Change record

Version	Date	Amendment details	Status
1	07 Nov 2018	New procedure	Withdrawn

	Jul 2020	Review date extended 6 months	
2	Mar 2022	Full revision. Flowchart added at 5.1. Mitigation of risk added. Clarity added that procedure also applies to new/changed information flows. Flowchart at 5.8 extended to include completion of screening questions. Roles and responsibilities updated. Example risks added at Appendix 3.	Withdrawn
2.1	31 May 2022	Section 5.6 added and 5.9 flowchart updated to reflect review of information flows	Approved
2.1	Sept 2024	Review date extended till 05 April 2025 to allow inclusion in wider review.	Published
2.1	May 2025	Review date extended till 30 Sept 2025	Published
2.1	April 2026	Review date extended till 31 Oct 2026	Published
2.1	19 Aug 2026	Review date extended till 31 Dec 2026	Published

Appendix 1 - Equality Analysis Screening Form

Section 1	Scope
Name of service area/directorate/department	Digital and Data Services
Title	Data Protection Impact Assessment Procedure
Type	Procedure/guidance
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:- • 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'.
Start date of Equality Analysis Screening	28 February 2022
End date of Equality Analysis Screening	29 March 2022

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Staff, patients, carers and family
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **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, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **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**
Describe any negative impacts	None
Describe any positive impacts	The Data Protection Act 2018 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.

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	Legislation, ICO guidance
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, 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.
If you answered No above, describe future plans that you may have to engage and involve people from different groups	

Section 4	Training needs
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

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 / Not applicable	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	

	Title of document being reviewed:	Yes / No / Not applicable	Comments
7.	**Implementation and monitoring**		
	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?	Y	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Y	
10.	**Publication**		
	Has the policy been reviewed for harm?	Y	
	Does the document identify whether it is private or public?	Y	Public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	y	

Appendix 3 – Example risks

Risks to individuals

i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
ii. Inadequate access controls increase the likelihood of information being accessed without a 'need to know'.
iii. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
iv. New surveillance methods may be an unjustified intrusion on their privacy.
v. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
vi. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
vii. Identifiers might be collected and linked which prevent people from using a service anonymously.
viii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
ix. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
x. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
xi. If a retention period is not established information might be used for longer than necessary.

Corporate risks

i. Non-compliance with the data protection legislation can lead to sanctions, fines and reputational damage.
ii. Problems which are only identified after the project has launched are more likely to require expensive fixes.
iii. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
iv. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
v. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
vi. Data losses which damage individuals could lead to claims for compensation.

Compliance risks

i. Non-compliance with the Data Protection Act 2018/General Data Protection Regulation (EU) 2016/679.
ii. Non-compliance with the Common Law Duty of Confidentiality.
iii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
iv. Non-compliance with sector specific legislation or standards.
v. Non-compliance with Human Rights Act 1998 and Equality Act 2010.

Clinical Safety Risks

The Standardisation Committee for Care Information standard SCCI0160 (Clinical Risk Management: Its Application in the Deployment and Use of Health IT Systems) requires Health

Organisations to establish appropriate procedures to ensure patient safety during the implementation and management of clinical information systems.

This means clinical risk analysis of using a clinical information system must be considered before deploying a new system or before implementing a significant change to an existing system, to ensure that the best design of the system and adequate team processes are employed in the use of the system in that particular service area.

If you are planning to implement a new clinical information system, making a significant change in an existing clinical information system for an existing service, or adding a new service to an existing clinical information system which may require changes to the system to accommodate the new service, please contact the organisation's Clinical Systems Team who can advise on what further clinical risk analysis needs to be considered for your proposed change