Torbay and South Devon NHS Foundation Trust

Data Protection Impact Assessment (Data Protection by Design) Policy

Document Information

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

Date of Issue:	February 2026	Next Review Date:	October 2026
Version:	5	Last Review Date:	February 2025
Author:	Information Governance Officer		
Director Responsible	Director of Corporate Governance & Trust Secretary		

Approval Route	
Approved By:	**Date Approved:**
Information Governance Operational Group	
Information Governance Steering Group	February 2025
Information Governance Steering Group	February 2024
Information Governance Steering Group	February 2023

Links or overlaps with other policies:

We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership.

We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy.

Amendment History

Issue	**Status**	**Date**	**Reason for Change**	**Authorised**
0.1	Draft	Sept 2020	New policy	Information Governance Steering Group
2	Final	July 2021	No change	Information Governance Steering Group
2.1	Final	Nov 2021	Removal of duplication	Information Governance Steering Group
2.2	Final	Feb 2023	No change	Information Governance Steering Group
3	Final	Feb 2024	Minor updates	Information Governance Steering Group
4	Final	Jan 2025	No change	Information Governance Steering Group
5	Final (this version)	Feb 2026	Update to assurance routes to reflect new Trust structures	Information Governance Operational Group

Contents

1. Introduction

1.1. It is important as an organisation that we are aware that the privacy of individuals is extremely important, and we must ensure that this is safeguarded. We must assure the public and ourselves that we have a robust process in place.

1.2. This Policy sets out the context of the Data Protection Impact Assessment within the Trust and provides an overarching guide on what this means to Trust staff. Further guidance is available in Data Protection Impact Assessment Guidance.

1.3. This policy applies to all staff working within the Trust who are responsible for the introduction of new processes or systems that are likely to involve a new use of personal data or significantly change the way in which personal data is handled.

2. Aims and objectives

2.1. For new projects or material changes to current Information Assets which may have an impact on the privacy of individuals, the Information Commissioners Office recommends that a Data Protection Impact Assessment is completed.

2.2. This document will provide information on the purposes of Data Protection Impact Assessments as well as details of what the process within the Trust entails.

3. Purpose

3.1. This Policy sets out the mandatory elements of Data Protection by Design. The data protection by design approach is an essential tool in minimising privacy risks and building trust.

3.2. Designing projects, processes, products or systems with data protection in mind at the outset can lead to:

- Identifying potential problems at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection concerns within the project
- Able to meet their legal requirements which leads to a reduced chance of any Data Protection and cyber security incidents.
- The project will not be stalled at a later point when producing information sharing protocols/agreements.

3.3. Data protection by design starts with the use of the Data Protection Impact Assessment.

3.4. The use of the Data Protection Impact Assessment is mandatory according to relevant Data Protection legislation (GDPR) Failure in compliance in relation to the use of the Data Protection Impact Assessment could lead to the Trust liable to enforcement actions from the Information Commissioner which includes fines.

3.5. Projects that require the adoption or installation of a computer system must consider data protection by design as a crucial element at all stages of the project.

3.6. All new computer-based processes will need an IT project form completed. The IT Tender document requires 3rd party suppliers to meet a minimum standard of information security including audit functionality and ability to report on who has accessed the information

4. Data Protection Impact Assessments (DPIAs)

4.1. All new or significantly changed processes or projects that involve Person Identifiable Data must comply with confidentiality, privacy and data protection requirements.

4.2. The DPIA is to assist in:

4.2.1. The identification of the project's privacy impacts

4.2.2. Understanding those impacts from the perspective of all stakeholders

4.2.3. An understanding of the acceptability of the project and its features by the organisations and people that will be affected by it

4.2.4. Identification and assessment of less privacy-invasive alternatives

4.2.5. Identification of ways in which negative impacts on privacy can be avoided

4.2.6. Identification of ways to lessen negative impacts on privacy • Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them

4.2.7. Documentation and publication of the outcomes.

4.3. The DPIA will describe the nature, scope, context and purpose of processing, assess the necessity, proportionality and compliance measures as well as identifying risks to individuals and measures to mitigate those risks.

4.4. DPIA must be completed for a change in collection, use and/or storage if personal data will be affected or for a project which could potentially affect personal data. Before completing the DPIA consideration must be given to changes in data processing which is likely to result in a high risk and may impact an individual's rights and freedoms.

5. DPIA Review and approval

5.1. If the project or process change involved Personal Identifiable Data (PID) the DPIA should be completed on the ICON page for Information Governance.

5.2. The IG Team will evaluate the information provided in the DPIA and will undertake a risk assessment on the proposed project or process change. This risk assessment will determine what further action is required. Any severe or catastrophic risks identified during this stage of the process will be escalated immediately as per the Trust's Risk Management Guidance and included on the relevant risk register and to the Trust's Caldicott Guardian

5.3. Completing the DPIA will be sufficient in demonstrating that all of the relevant privacy risks have been considered for the majority of projects or changes to existing processes. The outcome of the review by the IG team will then be sent back to the originator for their information and action.

5.4. In order to complete a DPIA the team may require evidence of the third parties information and cyber security, including but not limited to:

5.4.1. Business Continuity & Disaster Recovery plans

5.4.2. Cyber security certifications (Cyber Essentials / Cyber Essentials Plus, ISO27001 etc.)

5.4.3. Contracts

5.4.4. Data maps

5.4.5. Information Security Policies

5.4.6. Penetration testing reports

5.4.7. ICO registration

5.4.8. DSPT standards (when processing health and social care information)

5.5. Completion of a Digital Technology Assessment Criteria (DTAC) is also required for new digital health technologies and is part of the NHS Standard Contract.

5.6. In the event that an 'enhanced DPIA' needs to be undertaken, the IG Team will inform the originator and provide the document to be completed. High risk projects require the recommendation of the Trust's Caldicott Guardian / Data Protection Officer.

5.7. The outcome of these discussions will be included within the DPIA Report, which details the nature of the project or change, the issues and risks identified and what recommendations and actions are required. This report is then sent to the Trust's Senior Information Risk Owner (SIRO) who will review the information and will confirm whether or not the recommendations should be implemented.

5.8. The DPIA log will show a status of 'scored by IG' and risk scored documented once approved.

6. Responsibilities

6.1. The SIRO is ultimately responsible for reviewing the DPIAs for all systems or processes. This may be delegated to the Information Governance Team for low and medium risk projects.

6.2. The Data Protection Officer will provide specialist review where:
- 6.2.1. a legal basis for information processing has not been identified
- 6.2.2. the privacy risks associated with the processing would negatively impact the Trust
- 6.2.3. the processing involves a new or novel use of technology (including AI)
- 6.2.4. advice is required from the Information Commissioners Office

6.3. The Caldicott Guardian will provide specialist review where there are concerns the Caldicott principles may not have been met, or the processing involves a new or novel use of technology (including AI).

6.4. The Information Governance Team should:
- 6.4.1. Provide advice and support in the completion of the DPIA
- 6.4.2. Maintain the DPIA Log and provide regular reports to the Information Governance Steering Group
- 6.4.3. Review, update and implement the DPIA Policy
- 6.4.4. Review low and medium risk DPIAs
- 6.4.5. Escalate DPIAs requiring review by the SIRO, DPO or Caldicott Guardian

6.5. The Information Governance Operational Group:
- 6.5.1. Should receive DPIA log reports on a regular basis

6.6. Information Asset Owners are:
- 6.6.1. Responsible for ensuring that a DPIA is in place for their system(s) (if required)
- 6.6.2. Responsible for reviewing the DPIA when a process change is being made and amend the DPIA as appropriate.

6.7. Project Sponsor/Lead/Operational Managers are:
- 6.7.1. Responsible for ensuring that a DPIA is consulted upon by all interested parties.

6.8. The completion the online DPIA falls to a suitable project team member, Information Asset Owner or Operational Manager, depending upon whether the change is from a new project or process being implemented.

6.9. Assessment and scoring of the DPIA and any further checks which may be required will be completed by the Information Governance Team. Assistance may be sought by the IG Team from relevant stakeholders during the DPIA process.

6.10. The IG Team will complete the Statement of Assurance

6.11. For all new Business Cases the relevant Project Board should assure themselves that this policy has been taken into consideration during the project initiation phase. Projects likely to involve PID must complete a DPIA.

7. Data Protection by Design

7.1. Executive Summary

7.1.1. Data Protection by design is the concept where Data Protection is considered as a core aspect of a project or change management process which promotes privacy and data protection compliance from the start.

7.1.2. Data protection by design promotes meaningful data management and data quality throughout the information lifecycle. For example, when:

- Building and designing a new IT system for storing and accessing personal data
- Developing policy and strategies that have implications for privacy
- Implementing new data sharing initiatives
- Using data for any new or novel purposes

7.1.3. The Data Protection Impact Assessment (DPIA) is a mandatory tool as part of the data protection by design process. This approach ensures that privacy and data protection is a key consideration in the early stages of any project and then throughout its lifecycle.

7.1.4. It is important to ensure that as we progress with new and/or shared processes, services and systems that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality, or data protection requirements. In particular the confidentiality, integrity, and accessibility of personal information must be maintained, and such information must be processed safely and securely.

7.2. Review

7.2.1. DPIAs and the content of the Information Asset register will be reviewed for accuracy and reported via the Information Governance Operational Group (IGOG) to ensure Trust approved systems have appropriate assurance of the Data Protection by Design principle.

7.2.2. An audit of all elements that make up Data Protection by Design will be reviewed by Information Governance Operational Group annually.

7.3. Responsibilities

7.3.1. Article 25 specifies that, as the controller, organisations have responsibility for complying with data protection by design and by default. Depending on circumstances, there may be different requirements for different areas within the organisation. For example:

- senior management, e.g. developing a culture of privacy awareness and ensuring development of policies and procedures with data protection in mind.
- software engineers, system architects and application developers, e.g. those who design systems, products and services should take account of data protection

requirements and assist us in complying with our obligations
- our business practices, e.g. ensure that we embed data protection by design in all your internal processes and procedures

7.3.2. Data protection by design is about adopting an organisation-wide approach to data protection, and baking in privacy considerations into any processing activity we undertake.

7.3.3. The following roles are responsible for ensuring the accuracy of this document which is reviewed at Information Governance Operational Group:
- Trust Data Protection Officer (DPO)
- Caldicott Guardian
- Senior Information Risk Owner (SIRO)
- Data Security and Protection Lead

7.3.4. Information Governance team for assistance with completing the DPIA: tsdft.igteam@nhs.net and reviewing a projects compliance with the Data Protection by design principle.

7.3.5. IT projects for assistance with IT tender documents and IT projects view on the Trust's intranet.

8. Distribution

8.1. This policy document will be made available to staff via ICON, the Trust Website and signposted in the Staff Bulletin.

8.2. Awareness will be raised through Equality Impact Assessment training, all ratifying committees/groups, policies and procedures training and ICON.

9. Key Contacts

Contact	Email	Phone
Data Protection Officer	Tsdft.dpo@nhs.net	07393 799539
Information Governance Team	tsdft.igteam@nhs.net	01803 654868
Data Access & Disclosure Office	tsdft.dataprotection@nhs.net	01803 654868
Senior Information Risk Officer	tsdft.siro@nhs.net	
Caldicott Guardian	tsdft.caldicottguardian@nhs.net	
Freedom of Information Team	tsdft.foirequests@nhs.net	

10. Appendices

Appendix 1: Rapid Equality Impact Assessment

NHS
Torbay and South Devon
NHS Foundation Trust

Appendix 1
Rapid Equality Impact Assessment *(for use when writing policies and procedures)*

Policy Title (and number)	***Data protection by design (DPIA) policy***	**Version and Date**	*5*
Policy Author	Information Governance Officer		

An equality impact assessment (EIA) is a process designed to ensure that a policy, project or scheme does not discriminate or disadvantage people. EIAs also improve and promote equality. Consider the nature and extent of the impact, not the number of people affected.

EQUALITY ANALYSIS: How well do people from protected groups fare in relation to the general population?
PLEASE NOTE: Any 'Yes' answers may trigger a full EIA and must be referred to the equality leads below

Is it likely that the policy/procedure could treat people from protected groups less favorably than the general population? (see below)

Age	Yes ☐ No☒	Disability	Yes ☐ No☒	Sexual Orientation	Yes ☐ No☒
Race	Yes ☐ No☒	Gender	Yes ☐ No☒	Religion/Belief (non)	Yes ☐ No☒
Gender Reassignment	Yes ☐ No☒	Pregnancy/ Maternity	Yes ☐ No☒	Marriage/ Civil Partnership	Yes ☐ No☒

Is it likely that the policy/procedure could affect particular 'Inclusion Health' groups less favorably than the general population? (substance misuse; teenage mums; carers[1]; travellers[2]; homeless[3]; convictions; social isolation[4]; refugees)	Yes ☐ No☒
Please provide details for each protected group where you have indicated 'Yes'.	

VISION AND VALUES: Policies must aim to remove unintentional barriers and promote inclusion

Is inclusive language[5] used throughout?	Yes ☒ No☐
Are the services outlined in the policy/procedure fully accessible[6]?	Yes ☒ No☐
Does the policy/procedure encourage individualised and person-centered care?	Yes ☒ No☐
Could there be an adverse impact on an individual's independence or autonomy[7]?	Yes ☐ No☒
If 'Yes', how will you mitigate this risk to ensure fair and equal access?	

EXTERNAL FACTORS

Is the policy/procedure a result of national legislation which cannot be modified in any way?	Yes ☐ No☒
What is the reason for writing this policy? (Is it a result in a change of legislation/ national research?)	
To facilitate a standardized approach to policy documents across the Trust	
Who was consulted when drafting this policy/procedure? What were the recommendations/suggestions?	

ACTION PLAN: Please list all actions identified to address any impacts

Action	Person responsible	Completion date

AUTHORISATION:
By signing below, I confirm that the named person responsible above is aware of the actions assigned to them

Name of person completing the form	**Information Governance Officer**	**Signature**	
Validated by (line manager)	**Data Protection Officer**	**Signature**	

Any issues Please contact Diversity & Inclusion Lead
For Torbay and South Devon NHS Trusts, please email tsdft.diversityandinclusion@nhs.net

[1] Consider any additional needs of carers/ parents/ advocates etc, in addition to the service user
[2] Travellers may not be registered with a GP - consider how they may access/ be aware of services available to them
[3] Consider any provisions for those with no fixed abode, particularly relating to impact on discharge
[4] Consider how someone will be aware of (or access) a service if socially or geographically isolated
[5] Language must be relevant and appropriate, for example referring to partners, not husbands or wives
[6] Consider both physical access to services and how information/ communication in available in an accessible format
[7] Example: a telephone-based service may discriminate against people who are d/Deaf. Whilst someone may be able to act on their behalf, this does not promote independence or autonomy