Torbay and South Devon NHS Foundation Trust

Individual Information Rights 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:		Next Review Date:	June 2027
Version:	6	Last Review Date:	February 2026
Author:	Information Governance Officer		
Director Responsible	Director of Corporate Governance & Trust Secretary		

Approval Route	
Approved By:	**Date Approved:**
Information Governance Operational Group	
Information Governance Operational Group	February 2026
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	Feb 2026	Update to assurance routes to reflect new Trust structures	Information Governance Operational Group
6	Final (this version)	June 2026	Update to include a defined complaints procedure as required by the Data Use and Access Act.	Information Governance Operational Group

Contents

1. Introduction
2. Aims and objectives
3. Scope
4. Roles and responsibilities
5. Individuals' information rights overview
6. Right to be informed
7. Right of access
8. Right of access (deceased patients)
9. Right to rectification
10. Right of erasure
11. Right to data portability
12. Right to restrict data processing
13. Right to object
14. Right to not be subject to Automated Decision Making
15. Complaints
16. Failure to uphold information rights
17. Training
18. Distribution
19. Key Contacts/ Useful Links
20. Appendices

1. Introduction

1.1. This policy provides information about the rights of individuals with regard to their personal data held and processed by the Trust under data protection legislation – UK-GDPR and Data Protection Act 2018.

2. Aims and objectives

2.1. The aim of this policy is to support staff to understand their responsibilities in relation to the information rights of individuals whose personal data they process and to ensure the Trust complies with its legal obligations.

3. Scope

3.1. Every member of the Trust, including permanent staff, temporary staff, volunteers, contractors, Non-Executive Directors and anyone else who works on behalf of the Trust, has a legal obligation to maintain confidentiality and process personal data in accordance with current legislation.

3.2. Individuals who come into contact with the Trust have rights under law to ensure their data is kept secure. The UK GDPR and DPA 2018 enhance the information rights of individuals.

4. Roles and responsibilities

4.1. The Chief Executive has the ultimate responsibility for compliance with all relevant Acts and guidance within the Trust. They have delegated the responsibility for bringing data protection issues to the Board and SIRO.

4.2. The Data Protection Officer (DPO) is responsible for the following:

- Ensuring the Trust complies with all relevant Acts and Guidance in relation to Data Protection and Access
- Promoting Data Protection awareness throughout the Trust by providing written procedures/guidance that are widely disseminated and available to staff
- Co-ordinating the work of other staff with data protection responsibilities
- Ensuring patients and service users are provided with information on their rights under data protection legislation and how the information we collect is held, used, shared and stored
- Monitoring compliance with the Act and the effectiveness of procedures through the use of compliance checks/audits and ensures appropriate action is taken where non-compliance is identified
- Implement and maintain a process for handling Subject Access Requests including from patients, services users, and third parties, Solicitors, Courts and Police

4.3. Managers will ensure that all staff including contractors, bank, voluntary and other agencies staff will:

- Ensure that the contents of this policy are disseminated and discussed and that possible implications for service delivery are identified and acted upon.
- Ensuring staff within their area of responsibility are aware of this policy and comply with its requirements. Services are required to act promptly upon any request by an individual under this policy, whether received verbally or in writing, and to notify the DADO Team without undue delay, so the request can be formally logged and compliance with timescales monitored.

- Ensuring staff understand their responsibility and complete appropriate training to manage all requests for the following individuals' rights:
  - Right to be informed o Right of informal access to view records
  - Right to rectification
  - Right to erasure
  - Right to restrict processing
  - Right to data portability
  - Right to object

4.4. All Staff will be expected to:

- adhere to IG policies and any associated procedures and guidelines
- attend all mandatory training and awareness programs
- ensure that all personal identifiable information is accurate, relevant, up-to-date and used appropriately on both electronic and manual records and devices
- share information on a 'need to know' basis only
- ensure that all personal identifiable information is kept safe and secure at all times and in line with the Trust's Retention & Disposal Schedule
- recognise and appropriately signpost any information rights request

4.5. Data Access and Disclosure Office (DADO) will ensure that:

- all information rights requests are appropriately logged, responded to any actioned within a timely manner • compliance with statutory timescales is monitored
- all requests for records of deceased individuals handled under the Access to Health Records Act 1990

5. Individuals information rights overview

5.1.1. The Trust has a legal obligation to identify that an individual has made a request under the following rights and to handle it accordingly

- Right to be informed
- Right of access
- Right of rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related automated decision-making, including data profiling

5.1.2. The following provisions apply to all information rights:

- Requests can be made verbally or in writing - The individual does not need to specify the exact phrase relating to their request, eg 'right of access' or mention the relevant Article in the UK GDPR or reference the Data Protection Act. Verbal requests must be recorded and confirmed with the individual to ensure their request has been clearly understood.

- Requests must be acted upon without undue delay and responded to within one month - The time limit starts from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month, ie the day of receipt is day zero. For practical purposes and to comply with system requirements a 28-day period has been adopted by the Trust to ensure compliance is always within a calendar month.

- The identity of the individual needs to be confirmed before disclosing personal data - If there are doubts about the identity of the person making the request,

proof of ID must be requested. However, the individual must be told without undue delay that more information is needed from them to confirm their identity. The period for responding to the request begins when the identification information is received. If the person does not have ID, reasonable efforts will be made to establish identity.

- Requests are free of charge - Normally, requests will be processed and information provided, where applicable, free of charge. Where a request is considered to be 'manifestly unreasonable, unfounded, excessive, or repeated' a reasonable fee, based on the administrative cost only may be charged, or the request refused. In either case the decision will need to be justified.

- Refusal - If a request is refused, the individual must be informed without undue delay and within one calendar month. The refusal must include: the reason(s); the right to complain; the ability to request a review or seek legal remedy.

6. The rights to be informed

6.1.1. The right to be informed encompasses the obligation to provide clear and concise information regarding the collection and use of information, typically through a privacy notice. It emphasises the need for transparency over how the Trust uses personal data.

6.1.2. A Privacy Notice must include
- The personal information being collected
- The legal basis for processing
- What we do with the information
- Why we need the information
- Where the information is generated from
- Who we share information with
- How long we keep information

6.1.3. The Trust has an overarching privacy notice available in multiple formats and translated upon request. However, specific projects and information sharing beyond direct care purposes must have a local privacy notices.

6.1.4. Local privacy notices should be reviewed and approved by the IG Team as part of the DPIA process.

6.1.5. Template privacy notices are available upon request from the IG Team on tsdft.igteam@nhs.net

7. The right of access

7.1. The right of access is usually referred to as a Subject Access Request. This right allows access to a copy of personal data held by the Trust.

7.2. Requests to access information can be made either informally or formally.

7.2.1. Informal requests to access – Are where a person asks to view (but not take) a copy of information held about them. This also includes requests to access information previously provided, such as copies of letters already issued.
- It is the responsibility of the health professional in charge of the applicant's care to organise an appropriate viewing of information.
- The health professional should arrange suitable representation for the patient to

help understand any technical language or medical terminology they may have difficulty understanding in the records.

7.2.2. Formal requests to access – Are where a person requests a copy of information held about them. These requests are managed by the Data Access and Disclosure Office (DADO).

7.2.3. Any requests for copies of information relating to an individual and received from that individual (the data subject), their representatives (friends, family members or legal representatives), or other bodies not listed in the Public Interest Information Sharing Policy should be sent to the DADO Team (tsdft.dataprotection@nhs.net) for action.

8. Right to access (deceased patients)

8.1. Whilst not covered by UK data protection legislation, requests for access to medical information pertaining to deceased individuals falls under the Access to Health Records Act 1990.

8.2. The Trust is responsible for the confidentiality of patient information after a patient's death. As such, the need to maintain the individual's confidentiality remains with the Trust in the absence of the patient's consent.

8.3. The 1990 Act provides for an application to be submitted by: the patient's personal representative, and any person who may have a claim arising out of the patient's death

8.4. The personal representative is the only person who has an unqualified right of access to a deceased person's record and need give no reason for applying to access that record. They will either be an executor for the estate of a deceased person who left a Will, or the administrator of a deceased person who died intestate (without a Will). In either case a court will issue "letters testamentary", "letters of administration" or "letters of representation" stating that an executor or administrator has been appointed. This proof of authority plus a copy of the deceased's death certificate will be required prior to processing such a request, together with the proof of identity of the personal representative is required.

8.5. In line with the data protection legislation the right to access personal data is normally free of charge. The Trust has, therefore, decided to adopt the same approach for access to a deceased person's record.

8.6. More detailed guidance on the processing of requests for access can be found in the Subject Access Requests Procedure.

9. Right to rectification

9.1. Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Personal data is defined under Data Protection Act 2018 as inaccurate if it is factually incorrect or misleading as to any matter of fact.

9.2. There is no need for the data subject or their representative to specify they are exerting their 'right to rectification'. As long as the individual has challenged the accuracy of their data and has asked for it to be corrected or has asked that you take steps to complete data held about them that is incomplete this will be a valid request. If a request for rectification is received all reasonable steps should be taken to be satisfied that the data is accurate and to rectify the data if necessary.

9.3. All requests for rectification of medical information or information contained in a medical record should be submitted the Data Access and Disclosure Office on tsdft.dataprotection@nhs.net Requests for rectification of staff information may be managed by the appropriate line manager or Information Asset Owner.

9.4. When considering the individuals request, all arguments and evidence provided by the data subject should be taken into account. What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for.

9.5. Where the data in question records an opinion or medical information, this can be complex. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified. In these circumstances rectification can be refused.

9.6. Where rectification is refused, the individual's disagreement should be recorded. It is good practice to place a note on the system/record indicating that the individual challenges the accuracy and the reasons for this.

10. Right to erasure

10.1. The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and only applies in certain circumstances.

10.2. The right to erasure does not apply to information held for the provision of direct care.

10.3. Where information collected is not used for direct care purposes, for example, for research and publication, this request will be managed by the service and the request formally logged and monitored by the Trust's DADO Team.

10.4. There are some specific circumstances where the right to erasure does not apply, and you can refuse to deal with a request. The right to erasure does not apply if processing is necessary for one of the following reasons:

- to comply with a legal obligation; the right to erasure does not apply to health records, where a complete audit trail must be preserved.
- for the performance of a task carried out in the public interest or in the exercise of official authority - the right to erasure does not apply to health records as provision of healthcare is a public task.
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing – the right of erasure does not apply to health research; or
- for the establishment, exercise or defence of legal claims.

10.5. Data protection legislation also specifies two circumstances where the right to erasure will not apply to special category (sensitive) data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices) Public health screening and pandemic management; or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services).

11. Right to restrict processing

11.1. Individuals have a right to request restriction or suppression of processing their personal data. This is not an absolute right and applies in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. This request will be managed by the service and the request formally logged and monitored by the Trust's Data Access and Disclosure Office.

11.2. Processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Methods used to restrict the processing should be appropriate for the type of processing being carried out.

11.3. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information held or how it has been processed. In most cases the restriction of an individual's personal data will only be in place for a certain period of time and not indefinitely.

11.4. Individuals have the right to request restriction of the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and therefore processing is restricted whilst the accuracy is being verified
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead
- the personal data is no longer needed, but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has exercised their right to object to the processing of their data under Article 21(1), either: o where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller o where processing is necessary for the purposes of legitimate interests

11.5. When processing is restricted the personal data may be stored but not processed further; enough information about the individual must be retained to ensure that the restriction is respected in future; and individuals must be informed when a decision is taken to lift a restriction on processing, before the restriction is lifted.

11.6. A number of different methods can be used to restrict data, such as: temporarily moving the data to another processing system; making the data unavailable to users; or temporarily removing published data from a website.

11.7. A note should also be placed on the system that the processing of this data has been restricted.

12. Right to data portability

12.1. The right to data portability is limited to information that is held in a machine-readable format.

12.2. The right to data portability does not apply to information held for the provision of direct care.

12.3. This right does apply to telephone/video recordings, including CCTV footage, where it exists.

12.4. All requests under this right will be managed by the service and the request formally logged and monitored by the Trust's Data Access and Disclosure Office.

12.5. The right to 'data portability' only applies:

- to personal data an individual has provided to a Controller, i.e. data derived, inferred or created by the Controller is excluded;
- where the processing is based on the individual's consent or for the performance of a contract.; and
- when processing is carried out by automated means, i.e. paper records are excluded.

13. Right to object

13.1. This request will be managed by the service and the request formally logged and monitored by the Trust's Information Governance Team (tsdft.igteam@nhs.net).

13.2. Individuals who have an objection on "grounds relating to their particular situation" have the right to stop or prevent processing.

13.3. This right only applies in certain circumstances, and depends on the purpose for which the information was collected:

13.3.1. Absolute right: direct marketing
13.3.2. Not absolute right: task carried out in the public interest; exercise of official duty; legitimate interests
13.3.3. More limited – scientific / historical research / statistical purposes

13.4. The Trust has detailed guidance on management of the right to object available on the Intranet or by contacting the Information Governance department.

14. Right to not be subject to Automated Decision Making

14.1. The UK-GDPR has additional provisions on automated decision making and profiling of individuals.

14.1.1. Automated individual decision-making (making a decision solely by automated means without any human involvement). For example,

- a recruitment aptitude test which uses pre-programmed algorithms and criteria; and
- profiling (automated processing of personal data to evaluate certain things about an individual).

14.1.2. Profiling can be part of an automated decision-making process.

14.1.3. Because this type of processing is considered to be high-risk the UK GDPR requires a Data Protection Impact Assessment to be carried out show that risks have been identified, assessed what actions are necessary to address the risks associated with this type of processing.

14.1.4. This request will be managed by the service and the request formally logged and monitored by the Trust's Information Governance Team (tsdft.igteam@nhs.net).

14.1.5. All uses of AI must consider the right to not be subject to automated decision making and profiling.

15. Complaints

15.1. Complaints about the handling of personal data or any individual information rights are managed in accordance with the Trust's Data Protection Complaints Policy.

15.2. The Data Protection Officer will independently review and respond to any complaints made under this policy.

15.3. Where upheld, the Trust may take remedial action such as correcting data, improving processes, strengthening controls, providing training, or issuing an apology. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner's Office (ICO).

16. Failure to uphold information rights

16.1. In addition to monetary penalties, the UK GDPR gives the Information Commissioners Office different types of sanctions to help organisations comply with the obligations in regards to information rights. While these do not impose financial penalties, an organisation's reputation may suffer significantly.

16.2. All failures to uphold or facilitate information rights requests are monitored by the Trusts Information Governance Steering Group, and significant failings reported on the Trust's Incident Reporting System and to the Information Commissioners Office.

16.3. Performance figures relating to numbers of requests, the average turnaround times and compliance rates for statutory timescales are provided on a monthly basis as part of the Trust's Performance Report presented to the Information Governance Steering Group

17. Training

17.1. All staff will attend, as part of their induction, training sessions on Information Governance and additional annual training will be provided to all staff through a mandatory training online or face-to-face programme.

18. Distribution

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

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

19. 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	

20. Appendices

Appendix 1: Rapid Equality Impact Assessment

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

Policy Title (and number)	***Individual Information Rights Policy***	**Version and Date**	*6*
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