TRANSFER OF DATA POLICY

POLICY

Reference	IG 010	
Approving Body	Data Protection and Cyber Security Committee	
Date Approved	17th November 2025	
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**	
	YES	**NO**
	X	
Issue Date	January 2026	
Version	4	
Summary of Changes from Previous Version	Included: International Data Transfer Agreement requirements Transfer Risk Assessment tool Data (Use and Access) Act 2025 Data Subject complaints process	
Supersedes	3	
Document Category	• Information Governance	
Consultation Undertaken	• Information Governance Working Group • Data Protection and Cyber Security Committee	
Date of Completion of Equality Impact Assessment	10th November 2025	
Date of Environmental Impact Assessment (if applicable)	Not applicable	
Legal and/or Accreditation Implications	Ensure compliance with: UK General Data Protection Regulation Data Protection Act 2018 Data (Use and Access) Act 2025 Regulation of Investigatory Powers Act 2000 The Telecommunications (Lawful Business Practice) Regulations 2000 Privacy and Electronic Communications Regulations	
	Network and Information Systems Regulations 2018 (UK)	
Target Audience	All staff	
Review Date	2 years	
Sponsor (Position)	Director of Corporate Affairs	
Author (Position & Name)	Head of Data Security and Privacy, Jacquie Widdowson	
Lead Division/ Directorate	Corporate	
Lead Specialty/ Service/ Department	Information Governance	

Position of Person able to provide Further Guidance/Information	Head of Data Security and Privacy
Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Not applicable	
Template control	April 2024

Contents

1.0 INTRODUCTION

Being responsible for compliance with the UK GDPR and Data Protection Act means that we need to be proactive and organised about our approach to data protection. The Data (Use and Access) Act 2025 introduces new lawful bases for processing, enhanced transparency obligations, and expanded ICO powers. All data transfers must comply with the Data (Use and Access) Act provisions alongside UK GDPR and Data Protection Act 2018. The Data (Use and Access) Act introduces a new lawful basis ("recognised legitimate interest") for certain public interest activities that will be implemented and enforceable from June 2026. The policy will be updated as ICO guidance evolves.

This policy defines the process that will need to be undertaken by the transferring and receiving organisations prior to any data ownership being transferred from one legal organisation to another.

Taking responsibility for what we do with personal data, and demonstrating the steps we have taken to protect people's rights not only results in better legal compliance, but it also offers us a competitive edge. Accountability is a real opportunity for us to show, and prove, how we respect people's privacy. This can help us to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that we actively considered the risks and put in place measures and safeguards can help us provide mitigation against any potential enforcement action.

Personal confidential data (in paper and electronic form) are required to be included in the formal arrangements and agreements involved in transferring services to receiving organisations in order that the receiving organisation can perform its functions.

The responsibility for transferring records is determined dependent on whether the receiving organisation is a legal entity. The concept of Data Controller and Data Processor are also integral, as the Data Controller has responsibility for the use to which the data is put by an organisation and may undertake the processing, whilst a Data Processor may be a separate organisation that provides services to the Data Controller organisation.

This policy is issued and maintained by the Trust at the issue defined on the front sheet, which supersedes and replaces all previous versions.

2.0 POLICY STATEMENT

The purpose of this policy is to define the approach taken by the Trust in the legal transfer of data from one organisation to another. It sets out clear definitions, responsibilities, and process requirements to enable the principles and techniques of the transfer of data to be applied consistently throughout the organisation.

3.0 DEFINITIONS/ ABBREVIATIONS

Data Controller	The Trust is registered as a Data Controller with the Information Commissioner's Office. A Data Controller is defined as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed'.
Data Processor	A processor is a natural or legal person (not an employee) public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.
Data Transfer Agreement	A data transfer agreement (DTA) is a legal document that lays out the terms and conditions of sending or receiving personal data to another jurisdiction or organisation. The agreement will include provisions for how data will be used and protected as a result of the transfer.
DUAA	Data (Use and Access) Act 2025
International Data Transfer Agreement (IDTA)	When personal data is to be transferred outside the UK, staff are required to utilise the International Data Transfer Agreement and Addendum as the legal mechanism for such transfers
ICO (Information Commissioner's Office)	The ICO is the supervisory authority for data protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance, and take enforcement action where appropriate.
Personal data	Refers to information about a particular living individual 'data subject'. The classification of personal data depends on the recipient's ability to identify an individual from the information. It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data. It does not cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data. It only includes paper records if we plan to put them on a computer (or other digital device) or file them in an organised way. In the Trust, all paper records are technically included – but will be exempt from most of the usual data protection rules for unfiled papers and notes.

	Personal information encompasses a wide range of data that can be used to identify a living individual. Below are key examples outlining the types of personal information: • Name: The individual's name is a primary means of identification and is considered personal information. • Identification Number: This includes unique identifiers such as NHS numbers or National Insurance (NI) numbers, which are assigned to individuals for official purposes. • Location Data: Information that reveals the geographical position of an individual, either at a particular time or over a period, qualifies as personal data. • Online Identifier: Online data points such as IP addresses and cookie identifiers are also recognised as personal information, as they can be linked to specific individuals. • Factors Specific to Identity: Personal data includes details relating to physical, physiological, genetic, mental, economic, cultural or social identity that pertain to a natural person. These factors, individually or combined, can be used to distinguish or trace an individual's identity.
Processing	Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.
Special categories of personal information (or data)	The special categories of personal data are: a) racial or ethnic origin b) political opinions c) religious or philosophical beliefs d) trade-union membership e) genetic data f) biometric data for the purpose of uniquely identifying a natural person g) data concerning health h) data concerning a natural person's sex life or sexual orientation

4.0 ROLES AND RESPONSIBILITIES

Trust Board

The Trust Board is responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Data Protection and Cyber Security Committee
The Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

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 Data Protection and Cyber Security 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 Chief Medical Officer 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 Senior Information Risk Owner and works with 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 staff (including Medirest, Skanska, agency, and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties' staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of IG security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors. Any IG security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team.

All actual or suspected data breaches must be reported immediately in line with the Trust's Incident Reporting Policy. The Data Protection Officer will assess whether notification to the ICO and/or DSPT is required within 72 hours.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read, and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our policy and accept their personal responsibility to maintain confidentiality at all times.

5.0 APPROVAL

This policy is approved by the Data Protection and Cyber Security Committee.

6.0 CONTRACTS AND RESPONSIBILITITES FOR DATA PROCESSING

Whenever a data controller engages a data processor to manage personal data on their behalf, it is imperative that a formal written contract is established. This contract must set out, in clear terms, the responsibilities and liabilities of both the controller and the processor.

Under Article 24(1) of the UK GDPR, organisations are obligated to implement technical[1] and organisational measures that both ensure and demonstrate compliance with the UK GDPR. These measures should be risk-based and proportionate to the nature of the data processing activities being undertaken. Furthermore, such measures must be reviewed and updated as necessary to maintain ongoing compliance.

At a minimum, contracts between controllers and processors must include specific terms. These terms must require processors to act in a manner that ensures the security of processing, and to assist controllers in enabling individuals to exercise their rights under the UK GDPR. If a processor intends to employ another organisation, referred to as a sub-processor, to support the processing of personal data, then a written contract must also exist between the processor and the sub-processor.

Controllers must articulate their expectations for data processors explicitly within formal contracts. This requirement is applicable to all parties—including NHS organisations—and must always be fulfilled through formal contracts, rather than by relying on Service Level Agreements.

Such contracts should detail the following:

- The subject matter and duration of the processing
- The nature and purpose of the processing
- The types of personal data involved
- The categories of data subjects
- The obligations and rights of the controller

Additionally, contracts must contain specific terms or clauses addressing:

- Processing solely on the controller's documented instructions
- The duty of confidence
- Appropriate security measures
- The use of sub-processors
- Data subjects' rights
- Assistance to the controller
- End-of-contract provisions
- Audits and inspections

[1] require AES-256 encryption for data in transit and at rest, and regular review of security controls.

Compliance with the UK GDPR and the Data (Use and Access) Act (DUAA) calls for a proactive and organised approach to data protection. These contracts are fundamental in establishing clear expectations for the services provided, and in ensuring mutual protection for all parties involved, given the liabilities associated with service delivery.

Legal arrangements for the transfer of data must be put in place between Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) and any receiving organisation. The transfer of records is to be treated as an integral part of the formal transfer of assets, alongside premises, staff, and hardware. Should the receiving organisation refuse to accept archived or historical data, responsibility for the continued existence, storage, and retention of those records must be clarified at the point of transfer, including any ongoing arrangements.

When multiple providers utilise a single instance of software to facilitate patient care across organisations, it is essential to establish information sharing protocols and confidentiality agreements. These measures ensure that information is shared and protected appropriately across all participating organisations.

6.1 TRANSFER OF DATA OWNERSHIP

If there is an intention to transfer data ownership to another organisation, reasonable notice must be provided to NHIS by either the receiving or transferring organisation. All intentions to transfer ownership of data between organisations in the UK must be documented using the Data Transfer Agreement which can be found in the Transfer of Data Procedure.

Prior to any transfer of data, the transferring organisation must specify exactly which data is to be transferred. It is the transferring organisation’s responsibility to identify, collate, and document all the information and data sets subject to transfer, as outlined in the Data Transfer Agreement which can be found in the Transfer of Data Procedure Appendix B.

Where data is to be transferred between legal entities, a Data Transfer Agreement (DTA) is required. Both the receiving and transferring organisations are responsible for ensuring that appropriate legal advice is obtained regarding the data transfer agreement, and this advice should be sought from the Information Governance team before any data is transferred.
The data transfer agreement must specify the data sets to be transferred and should include all data items that will be passed to the receiving organisation. The completed Data Transfer Agreement which can be found in the Transfer of Data Procedure should be submitted to the Information Governance and NHIS Digital Business Teams for review prior to any action being taken.

Following completion and Data Protection Officer approval, the Data Transfer Agreement should be securely retained as part of the Trust’s official records. These documents may be subject to review by the ICO during audits or investigations

Any legal obligations that require continued access to data following the end of a contract (for instance, when care provision transitions from one provider to another) must be clearly stated at the outset of the contractual relationship. It should also be specified that data controller responsibilities will be retained for records generated during the contract period, particularly in cases where there is an ongoing potential for litigation against the provider of care.

6.2 INTERNATIONAL DATA TRANSFERS

The Information Commissioner's Office (ICO) has introduced the International Data Transfer Agreement (International Data Transfer Agreement) and Addendum, which have now replaced the former standard contractual clauses for international data transfers. These updated documents incorporate the implications of the binding decision handed down by the European Court of Justice in the "Schrems II" case.

When personal data is to be transferred outside the UK, staff are required to utilise the International Data Transfer Agreement and Addendum as the legal mechanism for such transfers. Before any international data transfer is initiated, both the International Data Transfer Agreement and Addendum must be properly completed and submitted for review to the Information Governance team.

Following completion and Data Protection Officer approval, the International Data Transfer Agreement and Addendum should be securely retained as part of the Trust's official records. These documents may be subject to review by the ICO during audits or investigations. Staff must ensure that they access and complete the appropriate templates for the International Data Transfer Agreement and Addendum, which are available in the Transfer of Data Procedure Appendix C.

6.3 TRANSFER RISK ASSESSMENTS

A Transfer Risk Assessment (TRA) is required for all restricted transfers of personal data outside the UK, to ensure that the transfer mechanism provides appropriate safeguards and that data subjects' rights remain protected in the destination country.

A Transfer Risk Assessment (TRA) is required:

- For any transfer of personal data to a country outside the UK that is not covered by an adequacy decision.
- When using the International Data Transfer Agreement (IDTA) or Addendum as the transfer mechanism.
- Before entering into any new international data sharing arrangement or renewing an existing one.

A Transfer Risk Assessment must be properly completed and submitted for review to the Information Governance team. Following completion and Data Protection Officer approval, the Transfer Risk Assessment should be securely retained as part of the Trust's official records before any restricted transfer takes place. These documents may be subject to review by the ICO during audits or investigations. The scope must be reasonable and proportionate. This should take into consideration the risk to people inherent in the data being transferred, the amount of data being transferred, and the size of the controller or processor making the restricted transfer, and so the resources available to it.

The template is available in the Transfer of Data Procedure Appendix D.

6.4 DATA USE REGISTER

The Trust will maintain a Data Use Register documenting all instances of data access and sharing, including purpose, legal basis, recipients, and retention periods, in compliance with Data (Use and Access) Act (DUAA) transparency requirements.

6.5 TRANSFER OF DATA TO NHS ENGLAND

Secure Electronic File Transfer (SEFT)
Secure Electronic File Transfer (SEFT) works by providing a secure wrapper around any file, regardless of its size, structure, or data content. SEFT provides data security during transmission (by using a 256-bit AES encryption mechanism). The data are held in secure containers at NHS England and only people who are authorised to process the data are allowed access.

SEFT can only be accessed by registered and approved users. NHS England will invite relevant people to register for the service and send you log-in details. Further information is available here. If you have any problems with your transfers please send an email to seft.team@nhs.net.

6.6 HANDLING DATA SUBJECT COMPLAINTS

The Trust is committed to resolving data protection concerns promptly and transparently.

- If you have concerns about how your personal data has been processed or transferred, you may raise a complaint with us by contacting the Information Governance Team sfh-tr.information.governance@nhs.net.
- We will acknowledge your complaint within **5 working days** and aim to provide a full response within **30 calendar days**.
- If you remain dissatisfied after our review, you have the right to escalate your complaint to the Information Commissioner's Office (ICO).
- Details on how to complain to the ICO are available at: https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/

- All complaints and outcomes will be logged and reviewed as part of our compliance monitoring under Data (Use and Access) Act (DUAA) and UK GDPR.

6.7 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A Data Protection Impact Assessment (DPIA) is a legal requirement that must be completed prior to any transfer of data. Conducting a DPIA serves to minimise potential data protection risks to individuals by identifying and addressing privacy concerns before data processing begins. 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. It is important to periodically review and reassess the Data Protection Impact Assessment (DPIA), particularly if circumstances change.

An annual review of the Data Protection Impact Assessment (DPIA) is recommended. Further information is available in the Data Protection Impact Assessment (DPIA) policy and procedure.

The DPIA process enables the organisation to identify privacy risks and ensure they are mitigated to an appropriate level. This assessment is essential to confirm that data transfers are carried out securely and in accordance with relevant legislation and best practice.
For further details, please refer to the Data Protection Impact Assessment Policy.

7.0 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 (e.g verbal, formal report etc) and by who)**
All requests for the transfer of data ownership from the customer to a subsequent organisation will be logged into the call management software in use at NHIS and given a unique reference number and monitored with reference to the SLA. The Head of Data Security & Privacy to be notified and ensure a Data Protection Impact Assessment has been completed prior to transfer.	NHIS Digital Business Team; and Head of Data Security & Privacy (Data Protection Officer)	Audit	Annual	Information Governance Working Group Data Protection and Cyber Security Committee.

8.0 TRAINING AND IMPLEMENTATION

8.1 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[2] 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 General Data Protection Regulations (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.

8.2 Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[3]

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document is not subject to an Environmental Impact Assessment

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Data Protection Act 2018
- Data (Use and Access) Act 2025
- UK General Data Protection Regulation
- National Cyber Security Centre Guidance

Related SFHFT Documents:

- Information Security Policy

[2] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[3] https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/

- Data Protection, Confidentiality and Disclosure Policy
- Safe Haven Procedure
- Transfer of Data Procedure

11.0 KEYWORDS

Information, Data Protection, Archive, Backup.

12.0 APPENDICES

- Refer to list in contents table

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

EIA Form Stage One:

Name EIA Assessor: G Robinson		**Date of EIA completion: 10th November 2025**
Department: Information Governance		**Division: Corporate**
Name of service/policy/procedure being reviewed or created: Transfer of Data Policy		
Name of person responsible for service/policy/procedure: Head of Data Security and Privacy		
Brief summary of policy, procedure or service being assessed: Information for the correct transfer of data between organisations external to the Trust		
Please state who this policy will affect: Patients **(Please delete as appropriate)**		
Protected Characteristic	**Considering data and supporting information, could protected characteristic groups' face negative impact, barriers, or discrimination? For example, are there any known health inequality or access issues to consider? (Yes or No)**	**Please describe what is contained within the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening.** **Please also provide a brief summary of what data or supporting information was considered to measure/decipher any impact.**
Race and Ethnicity	No	Not applicable.
Sex	No	
Age	No	
Religion and Belief	No	
Disability	No	
Sexuality	No	
Pregnancy and Maternity	No	

Gender Reassignment	No	

Marriage and Civil Partnership	No	Not applicable.
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	No	

If you have answered 'yes' to any of the above, please complete Stage 2 of the EIA.

What consultation with protected characteristic groups including patient groups have you carried out? None.

None.

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.

No.

On the basis of the information/evidence/consideration so far, do you believe that the policy / practice / service / other will have a positive or negative adverse impact on equality? (delete as appropriate)

Positive			**Negative**			
High	**Medium**	**Low**	**Nil**	**Low**	**Medium**	**High**

If you identified positive impact, please outline the details here:

The policy is written 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.

EIA Form Stage Two:

Protected Characteristic	Please explain, using examples of evidence and data, what the impact of the Policy, Procedure or Service/Clinical Guideline will be on the protected characteristic group.	Please outline any further actions to be taken to address and mitigate or remove any in barriers that have been identified.
Race and Ethnicity		
Gender		
Age		
Religion		
Disability		
Sexuality		
Pregnancy and Maternity		
Gender Reassignment		
Marriage and Civil Partnership		
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)		

Signature: *I can confirm I have read the Trust's Guidance document on Equality Impact Assessments prior to completing this form*
Date: 10th November 2025

Please send the complete EIA form to the People EDI Team for review. **Please send the form to: sfh-tr.edisupport@nhs.net**