INFORMATION SHARING POLICY

POLICY

Reference	IG/003	
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	Thorough review undertaken and internal audit recommendations included	
Supersedes	3	
Document Category	Information Governance	
Consultation Undertaken	Information Governance Working Group	
Date of Completion of Equality Impact Assessment	6th October 2025	
Date of Environmental Impact Assessment (if applicable)	Not applicable	
Legal and/or Accreditation Implications	Potential non-compliance with UK GDPR/Data Protection Act 2018, Health and Social Care Act, Duty of confidence	
Target Audience	All staff	
Review Date	2027	
Sponsor (Position)	Director of Corporate Affairs	
Author (Position & Name)	Head of Data Security and Privacy	
Lead Division/ Directorate	Corporate	
Lead Specialty/ Service/ Department	Information Governance	
Position of Person able to provide Further Guidance/Information	Information Governance Team	
Associated Documents/ Information		**Date Associated Documents/ Information was reviewed**

1. Data Protection, Confidentiality and Disclosure Policy 2. Data Protection, Confidentiality and Disclosure Procedure	July 2025 July 2025
Template control	April 2024

Contents

1.0 INTRODUCTION

Government policy underscores the importance of sharing information across organisational and professional boundaries. This approach is essential to achieve effective co-ordination and integration of services, particularly within the health and social care sectors.

The Caldicott Review, titled 'To share or not to share', highlighted that the duty to share information can be as significant as the duty to maintain patient confidentiality. Health and social care professionals are encouraged to share information in the best interests of their patients, provided this is done in accordance with the Caldicott principles. To facilitate this, professionals should feel supported by the policies of their employers, as well as guidance from regulators and professional bodies.

The Government has also stressed the importance of robust data practices. The Review of Data Security, Consent and Opt-Outs, published by the National Data Guardian in 2016, introduced ten Data Security Standards. These standards are integral to the annual self-assessment process using the Data Security and Protection Toolkit.

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), organisations are required to be accountable and able to demonstrate compliance with data protection legislation. This includes establishing systems and processes that protect and safeguard person-identifiable information, in line with both legal requirements and NHS mandatory standards. This also offers assurance to patients and the public regarding the use of their data.

All staff working in the NHS, including colleagues from Medirest, Skanska, agency staff, and contractors, are bound by the common law duty of confidence and must comply with data protection legislation. Handling personal information lawfully and compliantly is not only a contractual obligation but also a legal requirement. Staff should be aware that, under the DPA 2018, it is a criminal offence to knowingly or recklessly obtain or disclose personal data inappropriately. Further information is provided in Appendix 2.

This policy outlines the requirements for all Trust staff when sharing personal information, both within the NHS and with external bodies. The Information Commissioner's Office (ICO) has issued a data sharing code of practice, which must be followed whenever personal data is shared. The key legal and NHS-mandated frameworks guiding information sharing are detailed in Appendix 2.

2.0 POLICY STATEMENT

The sharing of information with other agencies plays a crucial role in supporting the Trust's activities, such as ensuring continuity of patient care. Nevertheless, both data protection legislation and the common law duty of confidentiality require organisations to give careful consideration to the following aspects before sharing information:

- What information is being shared
- With whom the information is shared
- The specific purpose for which the information is shared.

Failure to establish effective arrangements for sharing information can result in enforcement action and damage to the Trust's reputation.

Good Practice for Information Sharing

- Establish an information sharing agreement with any organisation with which personal information is routinely shared. These agreements must be reviewed or updated at least annually, regardless of whether there have been changes in sharing practices.
- Comply with the Information Commissioner's data sharing code of practice at all times.
- Share only the relevant patient information required to support patient care.
- Ensure that clear procedures exist for the transfer, retention, and deletion of information.

What to Avoid

- Do not share more personal information than is necessary for the intended purpose.
- Do not use identifiable personal information when the objective can be met by sharing anonymised data.
- Do not overlook the requirement to inform patients that their information is being shared.

The Trust is committed to ensuring that the sharing of personal information is governed by clear and transparent procedures that comply with legal and confidentiality obligations. Additionally, the Trust expects that routine sharing of personal information will be supported by an appropriate information sharing agreement and/or contract.

For the purposes of this policy, information sharing refers to the routine disclosure or receipt of personal information by the Trust, either individually or jointly, to or from another organisation or organisations. This process can include several different forms of information exchange, each supporting collaborative working and ensuring effective management of personal data.

Common Exchange of Information:

- The regular sharing of information between the Trust and another organisation, where data flows in both directions to facilitate mutual understanding and support.
- Provision of Information to Third Parties:
- One or more organisations may provide information to a third party or multiple third parties, as part of their operational or collaborative requirements.
- Pooling of Information Among Organisations:
- Several organisations may combine their information, making it accessible to each other. This approach supports joint initiatives and ensures all parties have the necessary data.

- Pooling of Information for Third Parties:
- In some instances, multiple organisations may pool information and then make it available to one or more third parties, depending on the needs of the collaboration or project.

Routine Processing of Personal Data
Information sharing also encompasses the regular processing of personal data by the Trust. This may involve joint or individual data controllers working together to support joint working enterprises, ensuring that personal information is managed appropriately to meet operational objectives.

Exceptional Circumstances
In addition to routine sharing, there may be exceptional, one-off disclosures of data. These occur in unexpected or emergency situations, where the sharing of information is necessary to address immediate concerns or risks.

3.0 DEFINITIONS/ ABBREVIATIONS

Implied consent: If confidential patient information is accessed and used for individual care then consent is implied, without the patient having to explicitly say so. Implied consent is only valid for direct care. This is because it is reasonable for patients to expect that relevant confidential patient information will be shared with those caring for them on a need to know basis.

Explicit consent: If confidential patient information is used for purposes beyond individual care, for example a research project, then it will normally be necessary for staff to obtain explicit consent. This is a very clear and specific statement of consent. It can be given in writing, verbally or through another form of communication such as sign language.

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.

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

This does not include personal data about criminal allegations, proceedings or convictions, separate rules apply. For further information please see the ICO link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/criminal-offence-data/.

Confidential information can be anything that relates to patients, staff or any other information (such as medical and staff records, contracts, tenders, etc.) held either in paper, disc, computer file or printout, video, photograph or even heard word of mouth. It includes information stored on portable devices such as laptops, mobile telephones and external hard drives/memory sticks). It can take many forms including patient level health information, employee records, occupational health records etc.

4.0 ROLES AND RESPONSIBILITIES

Committees

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 SIRO, 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 SIRO 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 IG policies and procedures are followed, recognise actual or potential IG 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 DPO 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 DOCUMENT REQUIREMENTS

6.1 Sharing of non-personal information

Not all information sharing involves personal data. In certain instances, only data that cannot be used to identify any individual—such as statistics, anonymous or aggregated numbers—is shared. This approach is commonly utilised both within the organisation and with external bodies.

Anonymous or aggregated information may be shared for a variety of purposes, including:

- Improving patient experience
- Facilitating the commissioning of services
- Managing and planning future services
- Supporting quality improvement and clinical leadership
- Assuring and enhancing the quality of care and treatment
- Fulfilling statutory returns and meeting data requests
- Training staff
- Auditing performance.

When sharing non-personal information, it is essential to adhere to the guidance set out in the document Anonymisation Standard for Publishing Health and Social Care Data Specification. This document outlines the necessary steps for selecting an appropriate anonymisation plan and for conducting risk assessments regarding the potential for re-identification. For additional guidance, reference should be made to the Information Commissioner's Office (ICO) anonymisation code of practice.

6.2 Sharing Personal Information with Other Organisations

Personal information may be shared with other organisations when it is necessary and proportionate, for instance, to investigate complaints or potential legal claims, protect children and adults at risk, or assess the need for service delivery and treatment. This policy outlines two primary types of information sharing: systematic, routine sharing and exceptional, one-off decisions.

Types of Information Sharing

- **Systematic, Routine Information Sharing**: This involves the regular sharing of the same data sets between the same organisations for an established purpose. It may also include arrangements where multiple organisations agree to pool their data for specific objectives.
- **Exceptional, One-Off Information Sharing**: While much sharing occurs in a planned and routine manner, there are instances where departments or staff must make ad-hoc decisions to share information outside existing agreements. These situations may arise in emergencies or where urgent sharing is required. All such decisions must be carefully considered and fully documented.

Factors to Consider When Sharing Personal Data

- Objectives of Sharing: Clearly define what the sharing intends to achieve. Consider whether the objective could be fulfilled without sharing personal data or by using anonymised information. Personal data should not be used for planning service provision if non-personal data suffices.
- Data to be Shared: Only share the specific data items required to accomplish the objectives. Adhere to the third Caldicott principle: "Use the minimum necessary personal confidential data."
- Access Requirements: Apply 'need to know' principles. Ensure that access to shared personal data is restricted to individuals who require it for their role, both internally and externally, and that onward sharing is appropriately limited.
- Timing of Sharing: Document whether sharing is ongoing and routine or triggered by specific events.
- Method of Sharing: Establish and follow robust security protocols for the transmission and access of data, supported by common security rules.
- Evaluating Effectiveness: Regularly assess whether the sharing arrangement continues to meet its objectives and that safeguards remain proportionate to the risks.
- Informing Individuals: Ensure individuals are provided with fair processing information as required by the GDPR, and that their rights, including access to shared information, are respected.
- Risk Assessment: Consider potential risks to both individuals and the organisation, such as possible harm, objections, or impacts on trust. Determine if the data is subject to the National Data Opt-out Programme and take care not to share data where a patient has exercised this right. Refer to the NHS England website and the Trust's National Data Opt-Out Policy for further information.
- Legal Basis: Establish the lawful basis for processing personal data (e.g. fulfilling statutory duties), and, where necessary, identify the condition for processing special categories of data (such as managing a health and care service).
- Common Law Duty of Confidence: If information is confidential, confirm the legal basis for disclosure, whether by consent (implied or explicit), overriding public interest, or legal requirement or permission.

Documentation and Escalation

It is essential to document all decisions and rationale related to information sharing. Where uncertainty or risk arises, staff must escalate the issue to the Information Governance Team at sfh-tr.information.governance@nhs.net.

For direct care purposes, consult the Caldicott Guardian; for non-care purposes, involve the Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO). All decisions, including legal basis and any guidance received, must be recorded and retained for audit purposes. For further assistance, staff should contact the Information Governance Team if unsure when it is appropriate to share information.

Staff Responsibilities When Sharing Information

- Ensure all information sharing complies with legislation, follows best practice, and is governed by a suitable information sharing agreement.
- Share only the minimum information necessary for the stated purpose.
- Respect the rights of individuals, including confidentiality, data security, and those rights established by UK GDPR.
- Uphold confidentiality unless there is a compelling public interest or legal justification for disclosure.
- Undertake annual reviews of information sharing arrangements to confirm that they continue to meet objectives and obligations.

Example: Can I share information outside the health system?

You should share information that is necessary to support the provision of individual care, including care provided by those who have not traditionally been considered to be health professionals. For example, you should share relevant parts of a person's health and care record with a social worker or care home manager where needed to support that person's care. The person's consent can be implied because they understand the information is being shared to support their care. In the same way, social care staff should share the relevant parts of a person's social care record with healthcare staff, when needed to support their care.

Scenario: A patient is admitted and is unable to communicate due to their medical condition. The next of kin requests an update on the patient's condition and care plan.

Steps for Staff:

1. **Check Capacity and Wishes:**
   - Does the patient have capacity to consent?
     - If yes, seek explicit consent from the patient before sharing.
     - If no, proceed to step 2.
   - Are there any known patient wishes about sharing with next of kin, for example are they documented in the case notes?
     - If yes, respect these wishes.

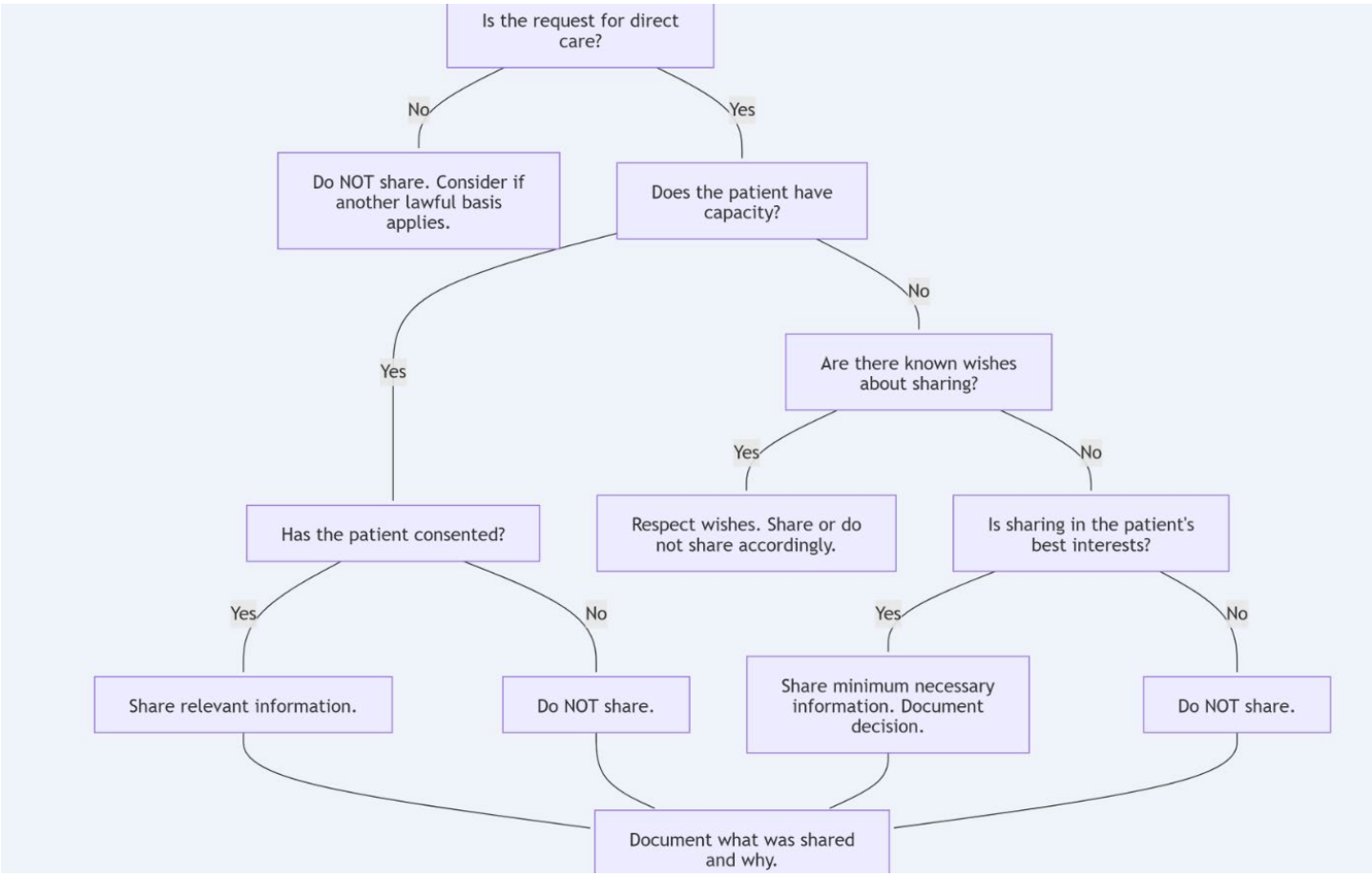
2. **Assess Best Interests:**
   - If the patient lacks capacity and there are no objections, share relevant information with the next of kin if it is in the patient's best interests.

3. **Minimum Necessary:**
   - Only share information necessary for the next of kin to support the patient's care.

4. **Document:**
   - Record the rationale for sharing, what was shared, and with whom, in the patient's record.

5. **Escalate if Unsure:**
   - If there is any doubt, consult the Caldicott Guardian or Information Governance Team.

Decision Tree



6.3 Sharing Information for Non-care Purposes

There are circumstances in which confidential personal information must be disclosed for purposes that do not relate directly to patient care. Whether information is being shared with a "trusted organisation" or otherwise, it is imperative that the purposes for such sharing are clearly documented and restricted solely to those specified purposes. In addition to this, further requirements may be necessary—such as obtaining documented consent or acquiring evidence of support under Section 251 of the NHS Act 2006—to ensure that the sharing of information is lawful.

Specifically, sharing information for 'non-care purposes'—often termed secondary uses, including but not limited to commissioning, healthcare development, and initiatives aimed at improving NHS resource efficiency—must adhere to all relevant NHS England guidance.

No confidential patient information may be disclosed for non-care purposes unless one of the following conditions is satisfied: explicit patient consent has been obtained, there is support under Section 251 of the NHS Act 2006, or it has been confirmed that the National Data Opt-out does not apply.

The Caldicott Report and its 2013 Review emphasise the importance of developing information sharing agreements between organisations that exchange personal identifiable information. When it is determined that an Information Sharing Agreement is necessary, staff should use the template provided by the Information Governance department.

If there is any uncertainty or risk associated with the proposed information sharing, staff are required to escalate the matter to the Information Governance Team. For direct care purposes, the Caldicott Guardian should be consulted. For all non-care purposes, the Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO) must be involved in the decision-making process. All decisions relating to information sharing—including the rationale, legal basis, and any advice received from the Information Governance Team, DPO, or Caldicott Guardian—must be fully documented and retained for audit purposes.

6.4 Information Sharing Agreements

Information sharing agreements, which may also be referred to as 'Information sharing protocols' or 'data sharing protocols', establish a unified set of rules for all organisations participating in an information sharing initiative. These agreements can form part of a contract between organisations, and their presence is considered good practice—especially where information is shared on a large scale or with regular frequency. It is recommended that such agreements are reviewed annually to ensure ongoing relevance and compliance.

Key Elements of an Information Sharing Agreement

- Purpose of Sharing: Clearly state the reason(s) for sharing information, outlining the specific objectives to be achieved.
- Legal Basis under DPA2018/UK GDPR: Identify the legal grounds that permit the sharing of information in accordance with the Data Protection Act 2018 and UK GDPR requirements.
- Common Law Duty of Confidence: Set out the legal basis for ensuring compliance with the common law duty of confidence.
- Potential Recipients: Specify the individuals or types of organisations that may receive the information, along with the circumstances under which access will be granted.

- Data Controllers and Processors: Clearly define which organisations are acting as data controllers and any parties fulfilling data processor roles.
- Data to be Shared: Detail the specific data items that are to be shared amongst the parties.
- Data Quality: Provide assurance regarding the accuracy, relevance, and usability of the data being shared.
- Data Security: Set out the measures in place to protect the data during transfer and handling.
- Data Retention: Define how long shared data will be retained and the arrangements for its secure disposal.
- Individuals' Rights: Outline procedures for handling subject access requests and other rights afforded under GDPR, as well as mechanisms for managing queries and complaints.
- Review and Termination: Describe how the effectiveness of the agreement will be reviewed and the process for its termination if required.
- Obligations and Assurance: Specify the standards expected of all parties, including sanctions for non-compliance or breaches by individual staff members.

A template information sharing agreement is available from the Information Governance department.

6.5 Information Sharing Agreements and Data Processing Agreements

When the Trust, in its capacity as a data controller, shares information directly with other organisations, it is essential to establish an information sharing agreement. This is required when the recipient organisation will act either jointly as a data controller alongside the Trust, or as an independent data controller for the information being shared. Such agreements formalise the terms under which personal data is exchanged and clarify each party's responsibilities in relation to the data.

In circumstances where an external organisation, such as a supplier, processes personal data solely on behalf of the Trust, this relationship must be governed by a data processing agreement, rather than an information sharing agreement. The UK General Data Protection Regulation (UK GDPR) stipulates that a binding contract or other legal act must be in place between the Trust (as data controller) and the processor. This contract should clearly define the subject matter and duration of the processing, the nature and purpose of the processing activities, the categories of personal data and data subjects involved, as well as the obligations and rights of the data controller.

6.6 Data Protection Impact Assessment

Before establishing a new process that involves processing of personal data including information sharing, a data protection impact assessment (DPIA) must be conducted. This is a legal requirement under the UK GDPR where there may be a high risk to individuals.

A Data Protection Impact Assessment (DPIA) can cover a single processing operation, or a group of similar processing operations. You may even be able to rely on an existing Data Protection Impact

Assessment (DPIA) if it covered a similar processing operation with similar risks. A group of organisations can also do a joint Data Protection Impact Assessment (DPIA) for a group project or industry-wide initiative. You should not view a Data Protection Impact Assessment (DPIA) as a one-off exercise to file away.

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.

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)**
DSPT validation	360 Assurance	Audit	Annually	IG Working Group / Head of Data Security & Privacy / DPO/Audit and Assurance Committee/Data Protection and Cyber Security Committee
Adherence to IG policies and procedures in nominated Division	360 Assurance	Audit	Annually	IG Working Group / Head of Data Security & Privacy / DPO/Audit and Assurance Committee/Data Protection and Cyber Security Committee
IAO report to the SIRO	IAO	Self-assessment return	Annually	Head of Data Security & Privacy / DPO/SIRO/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[1] 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.[2]

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:

- Confidentiality: NHS Code of Practice https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
- Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Data (Use and Access) Act 2025 https://www.legislation.gov.uk/ukpga/2025/18/contents
- Health and Social Care Act 2012 http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

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

- Human Rights Act 1998 https://www.legislation.gov.uk/ukpga/1998/42/contents
- Information: To share or not to share? The Information Governance Review March 2013 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
- NHS Act 2006 https://www.legislation.gov.uk/ukpga/2006/41/contents
- NHS Care Record Guarantee
- NHS Constitution https://www.gov.uk/government/publications/the-nhs-constitution-for-england
- UK General Data Protection Regulation Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

Related SFHFT Documents:

- Corporate Records Policy
- Data Protection Impact Assessment Procedure
- Data Protection, Confidentiality and Disclosure Policy
- Data Protection, Confidentiality and Disclosure Procedure
- Data Quality Policy
- Health Records Management Policy
- Information Security Policy

11.0 KEYWORDS

Caldicott, security, appropriate.

12.0 APPENDICES

- Please refer to the contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

EIA Form Stage One:

Name EIA Assessor: G Robinson	**Date of EIA completion:** 6th October 2025
Department: Information Governance	**Division:** Corporate
Name of service/policy/procedure being reviewed or created: Information Sharing Policy	
Name of person responsible for service/policy/procedure: Director of Corporate Affairs	
Brief summary of policy, procedure or service being assessed: Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), organisations are required to be accountable and able to demonstrate compliance with data protection legislation. This includes establishing systems and processes that protect and safeguard person-identifiable information, in line with both legal requirements and NHS mandatory standards. This also offers assurance to patients and the public regarding the use of their data.	
Please state who this policy will affect: Patients or Service Users, Carers or families, Commissioned Services, Communities in placed based settings, Staff, Stakeholder organisations.	

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	
Sex **Gender**	No	
Age	No	
Religion and Belief	No	
Disability	No	
Sexuality	No	
Pregnancy and Maternity	No	

Gender Reassignment	No	
Marriage and Civil Partnership	No	
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.

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.

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: G Robinson *I can confirm I have read the Trust's Guidance document on Equality Impact Assessments prior to completing this form*
Date: 6th October 2025
Please send the complete EIA form to the People EDI Team for review. **Please send the form to: sfh-tr.edisupport@nhs.net**

APPENDIX 2 – GUIDANCE ON THE LAW

There is no single source of law that regulates the powers that a public body (e.g. the Trust) has to use and to share personal information. The collection, use and disclosure of personal information are governed by a number of different areas of law. Some relevant legislation includes:

- the law that governs the actions of public bodies (administrative law).
- the Data Protection Act 2018.
- the UK General Data Protection Regulation.
- the Human Rights Act 1998 and the European Convention on Human Rights.
- the common law duty of confidence.

The interrelationship between the above areas of law is quite complex. The starting point is always to determine whether the Trust has the power to carry out any proposed data sharing. This will be a matter of administrative law.

The NHS Act[3] and the Health and Social Care Act define the Trust's functions in terms of its purposes, the things that it must do, and the powers which the Trust may exercise in order to achieve those purposes, the things that it may do. So it is necessary to identify where the data sharing in question would fit, if at all, into the range of things that the Trust is able to do. Broadly speaking, there are three ways in which it may do so:

1. **Express obligations** – Occasionally, a public body will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances but, where such an obligation applies, it is clearly permissible to share the information.

2. **Express powers** – Sometimes, a public body will have an express power to share information. Again, an express power will often be designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".

3. **Implied powers** – Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted. To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be "reasonably incidental" and then check that the organisation has the power to engage in that activity.

[3] https://www.legislation.gov.uk/ukpga/2006/41/section/43

All bodies must comply with the data protection principles. (See the Data Protection Act below).

It is also important to ascertain whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.

The next stage is then to consider whether the proposed data sharing might nevertheless be unlawful due under the Data Protection Act 2018, Human Rights Act 1998, or the common law tort of breach of confidence.

UK GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT 2018

The UK GDPR and DPA 2018 apply to living individuals and gives those individuals several important rights to ensure that personal data is processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing. Key principles in the UK GDPR and DPA 2018 that are relevant to information sharing are, personal information must be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
4. accurate and where necessary kept up to date.
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, and.
6. processed in a manner that ensures appropriate security of the personal data.
7. the UK GDPR also introduced the principle of accountability: The controller shall be responsible for and be able to demonstrate compliance with the principles.

The legislation gives rights to ‘data subjects’ including transparency (e.g. to be provided with privacy notices) and access to information held about them. There are other rights such as the right to object, which apply depending on the legal basis that applies.

Chapters 1 and 2 of the UK GDPR define these concepts:

‘Personal data’ ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘Pseudonymised data’ - The GDPR states clearly that pseudonymised data is ‘personal data’ and as a consequence the GDPR fully applies to pseudonymised data. However, the GDPR also states (in Recital 26) that data which is anonymised in such a way that individuals cannot be identified does not fall within the scope of the Regulation.

From this the important issue to be considered is around the fluid state of pseudonymisation. For example, if NHS England pseudonymises data and then goes onto make further use of that pseudonymised data, then in the eyes of the law the data will always be ‘personal data’; albeit once pseudonymised the law recognises this action as an increased form of protection/security. Ultimately though NHS England will have the key to the data and hence be capable of re-identifying the data.

However, if the same data set were to be disseminated to a third-party, then the data, on receipt, might not be classed as ‘personal data’. For this to be the case the data must be subject to controls (technical and legal) to ensure there is no reasonable likelihood of re-identification. If those conditions can be met, then the current ICO view is that this data is de-personalised in such a way that it falls out of the scope of the GDPR (and Data Protection Act 2018).

‘Special categories of personal data’ are personal data consisting of information as to racial or ethnic origin, political opinions, religious and similar beliefs, trade union membership, physical or mental health, sexual life, and the commission or alleged commission of any offence or criminal proceeding. The GDPR imposes additional requirements in relation to the processing (including the sharing) of such data.

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

‘**Controllers’** are persons who determine the purposes for which, and the manner in which, the personal data are processed.

Processors’ are persons who process personal data on the instructions of a controller for the controller’s purposes. They may not process the data for which they are instructed by the controller for their own purposes.

‘Data subjects’ are the individuals to whom the personal data relate.

OFFENCE OF UNLAWFUL OBTAINING OR DISCLOSURE

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

a) to obtain or disclose personal data without the consent of the controller

b) to procure the disclosure of personal data to another person without the consent of the controller, or

c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

HUMAN RIGHTS ACT 1998

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature. Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal data. Article 8 is not an absolute right – public authorities are permitted to interfere with it if it is lawful and proportionate to do so.

It is advisable to seek specialist advice if the disclosure or data sharing arrangement you are proposing engages Article 8 or any other Convention right. However, if you disclose or share personal data only in ways that comply with the DPA 2018 and common law duty of confidence, the sharing or disclosure of that information is also likely to comply with the HRA.

THE COMMON LAW DUTY OF CONFIDENCE

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client. It is irrelevant for example how old the patient/client is, or what the state of his/her mental health is; the duty still applies.

The Mental Capacity Act Code of Practice[4] gives guidance for decisions made under the Mental Capacity Act 2005. Staff should comply with this when information is to be shared about individuals who may lack capacity.

[4] https://www.england.nhs.uk/contact-us/pub-scheme/pol-proc/

The principle of Gillick competence[5] applies when considering a child's ability to consent to treatment and applies similarly to information sharing.

Three circumstances making disclosure of confidential information lawful are:

1. where the individual to whom the information relates has consented.
2. where disclosure is necessary for an overriding public interest such as to safeguard the individual, or others; or
3. where there is a legal duty to do so, for example a court order, or a permissive power such as Section 251 support under the NHS Act 2006.

Implied consent may be assumed where sharing of information for the purposes of providing direct care. However, this is only valid where appropriate information has been provided to the patient about the proposed sharing, or the activity is obvious – to ensure that the consent is informed.

Therefore, under the common law, a health or social care provider wishing to disclose a patient's/client's personal information to anyone outside the team providing care, or for non-care purposes should first seek the consent of that patient/client.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding safeguarding interest of the individual or others or in the public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. Solid justification is required before individual rights are set aside and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented.

Disclosures required by court order should be referred to the organisation's legal advisors as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested.

If a disclosure is made which is not permitted under common law the patient/client could possibly bring a legal action not only against the Trust but also against the individual responsible for the breach.

SECTION 251

Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes.

The Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' actually refer to approval given under the authority of the Regulations.

[5] https://www.nhs.uk/conditions/consent-to-treatment/children/

Section 251 was established to enable the common law duty of confidentiality to be set aside to enable disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent was not practical, having regard to the cost and technology available.

THE NHS CARE RECORD GUARANTEE

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant in relation to this policy is:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask, and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and
- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

Click here for an online link to NHS Care Record Guarantee[6]

Where there is any doubt, the Information Governance department can advise on whether a legal basis to share information exists.

[6] https://webarchive.nationalarchives.gov.uk/ukgwa/20131104121019/http://www.nigb.nhs.uk/pubs/nhscrg.pdf