Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

INFORMATION SHARING POLICY

POLICY

Reference	ISP-003		
Approving Body	Information Governance Committee		
Date Approved	14th April 2023		
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**	**N/A**
	x		
Issue Date	April 2023		
Version	3		
Summary of Changes from Previous Version	Thorough review undertaken and amendments have been in all sections		
Supersedes	2		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group		
Date of Completion of Equality Impact Assessment	21st March 2023		
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	April 2025		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Information Governance Manager and Data Protection Officer		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Governance Manager and Data Protection Officer		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
1. Data Protection and Disclosure Policy 2. Data Protection and Disclosure Procedure	March 2023
Template control	June 2020

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services.

The Caldicott Review 'To share or not to share' specified that **"The duty to share information can be as important as the duty to protect patient confidentiality". Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles. They should be supported by the policies of their employers, regulators and professional bodies.**

The Government has also emphasised the importance of data. The Review of Data Security, Consent and Opt-Outs published by the National Data Guardian in 2016 introduced ten Data Security Standards. These form the basis for the annual self-assessment of the Data Security and Protection Toolkit.

The UK General Data Protection Regulation (UK GDPR), and Data Protection Act 2018 (DPA 2018) requires organisations are accountable and able to demonstrate compliance.

It is important that the Trust protects and safeguards person-identifiable information that it gathers, creates processes and discloses, to comply with the law, relevant NHS mandatory requirements and provide assurance to patients and the general public.

An explanation of what is meant by information sharing can be found in section 4. All staff (including Medirest, Skanska, agency and contractor colleagues) working in the NHS are bound by the common law duty of confidence and must comply with data protection legislation. Staff must handle personal information they may come into contact with during the course of their work in a lawful and compliant manner. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation. It is important for staff to be aware that it is an offence under DPA 2018 for a person knowingly or recklessly to obtain or disclose personal data – see Appendix 2.

This policy sets out the requirements placed on all Trust staff when sharing personal information within the NHS and between the NHS and other bodies.

The Information Commissioner's Office (ICO) has issued a data sharing code of practice[1] that must be adhered to when sharing personal data.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-covered-by-the-code/

The Legal and NHS Mandated Framework for information sharing which forms the key guiding principles of this policy can be found in Appendix 2.

2.0 POLICY STATEMENT

The sharing of information with other agencies is necessary to support the Trust's activities. For example, to support continuity of patient care. However, data protection legislation and the common law duty of confidentiality place an obligation on organisations to consider carefully:

- what is shared
- with whom
- for what purpose.

Enforcement action and reputational damage are the consequences of not having effective information sharing arrangements in place.

Do...

- Put in place an information sharing agreement with organisations with whom we routinely share personal information
- Adhere to the Information Commissioner's data sharing code of practice[2]
- Share only relevant patient information with those supporting patient care.
- Ensure there are agreed transfer/retention/deletion processes in place.

Don't...

- Share more personal information than is necessary for the purpose.
- Use identifiable personal information if the purpose can be satisfied by sharing anonymised data.
- Forget that patients have a right to be told that we are sharing their information.
- Ignore changes to what is shared, and with whom; agreements should be periodically reviewed/updated.

The Trust will ensure that the sharing of personal information is governed by clear and transparent procedures that satisfy legal and confidentiality requirements.

Furthermore, the Trust expects that routine sharing of personal information will be supported by an appropriate information sharing agreement and/or contract.

[2] Available at: http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

3.0 DEFINITIONS/ ABBREVIATIONS

Information sharing – in the context of this policy means:

1. routine disclosure or receipt of personal information by the Trust, individually or jointly to or from another organisation or organisations. This can take the form of:

    - a common exchange of information;
    - one or more organisations providing information to a third party or parties;
    - several organisations pooling information and making it available to each other;
    - several organisations pooling information and making it available to a third party or parties.

2. routine processing of personal data by the Trust, jointly or as individual controllers, in support of their joint working enterprise

3. exceptional, one-off disclosures of data in unexpected or emergency situations.

Personal data means information about a particular living individual 'data subject'. 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.

Examples of personal information include:

- a name
- an identification number i.e. NHS number, NI number
- location data
- an online identifier ie. IP addresses and cookie identifiers
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/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 ultimately 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.

Information Governance 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 Information Governance 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 Medical Director 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.

Directors and Services Managers

Responsible for ensuring a comprehensive risk assessment is undertaken regarding the safety and security of the health records during transport to and from, and while present at non Trust premises. Completed risk assessments should be submitted to the Information Asset Owner for evaluation and approval by the Medical Records Advisory Group, also ensure that risk assessments are accurately maintained and risks re-evaluated and updated if significant changes are made to services.

Duty Nurse Managers

Out-of-hours or on occasions when the Caldicott Guardian, Information Governance Manager or Information Asset Owner are unavailable, Duty Nurse Managers in the first instance will be required to assume responsibility for any decision regarding urgent disclosures that cannot be delayed, they can if necessary seek assistance from staff involved in the Gold/Silver On-Call Protocol consulting with the Trust's Legal Advisors as necessary.

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.

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 Information Governance Committee.

6.0 DOCUMENT REQUIREMENTS

Sharing of non-personal information

Some information sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared.

Anonymous or aggregate (numbers) information may be shared internally or with other organisations for example to improve patient experience; facilitate commissioning of services; manage and plan future services; facilitate quality improvement and clinical leadership; assure and improve the quality of care and treatment; statutory returns and requests; train staff; audit performance.

Regard must be had to the document "Anonymisation standard for publishing health and social care data specification[3]" which specifies the steps required to select an appropriate anonymisation plan and to assess re-identification risk (refer to the ICO anonymisation code of practice[4] for further information).

Sharing personal information with other organisations

Necessary and proportionate, personal information may be shared with other organisations for example to investigate complaints or potential legal claims; protect children and adults at risk; assess need, service delivery and treatment.

This policy covers two main types of information sharing:

1. **systematic**, routine information sharing where the same data sets are shared between the same organisations for an established purpose; and
2. **exceptional**, one-off decisions to share information for any of a range of purposes.

Different approaches apply to these two types of information sharing and this policy reflects this. Some of the good practice recommendations that are relevant to systematic, routine information sharing are not applicable to exceptional, one-off decisions about sharing.

'Systematic' information sharing. This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

[3] https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data

[4] https://ico.org.uk/media/1061/anonymisation-code.pdf

Exceptional or 'one-off' information sharing. Much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments/staff may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation. All ad-hoc or one-off sharing decisions must be carefully considered and documented.

Factors to consider. When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you should consider **what is the sharing meant to achieve?** There should be a clear objective or set of objectives. Being clear about this will identify the following:

- **Could the objective be achieved without sharing the data or by anonymising it?**
  It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- **What information needs to be shared?**
  You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies "Use the minimum necessary personal confidential data".

- **Who requires access to the shared personal data?**
  You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations, individuals should only
  have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- **When should it be shared?**
  Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

- **How should it be shared?**
  This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- **How can we check the sharing is achieving its objectives?**
  You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- **How are individuals made aware of the information sharing?**
  Have individuals been provided with the fair processing information as required by the GDPR? How is it ensured that individual's rights are respected and can be exercised e.g. how can they access the information held once shared?

- **What risk to the individual and/or the organisation does the data sharing pose?**
  For example, is any individual likely to be damaged by it?
  Is any individual likely to object?
  Might it undermine individuals' trust in the organisations that keep records about them?

- **Is the information subject to the National Data Opt-out Programme?**
  If a patient has exercised their rights under this programme, care must be taken not to share that data. Further information can be found on the NHS England website and our procedure here[5].

- **What is the legal basis for data protection purposes?**
  Organisations must identify the lawful basis (e.g. meeting statutory duties) for processing and, where necessary, a condition for processing special categories data (e.g. managing a health and care service).

- **If the information is confidential**, what is the legal basis that complies with the common law duty of confidence? This can be consent (implied[6] or explicit[7]), overriding public interest or required or permitted by law.

It is good practice to document all decisions and reasoning related to the information sharing.

For any assistance and guidance, and if in any doubt about when it is appropriate to share information please contact the Information Governance team sfh-tr.information.governance@nhs.net.

In all circumstances of information sharing, staff will ensure that:

- When information needs to be shared, sharing complies with the law, guidance, best practice is followed and an information sharing agreement is in place;
- Only the minimum information necessary for the purpose will be shared;

[5] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=12805

[6] If confidential patient information is accessed and used for individual care then consent is implied, without the patient having to explicitly say so. 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.

[7] 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.

- Individuals' rights will be respected, particularly confidentiality, security and the rights established by the UK GDPR;
- Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure;
- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

Information Sharing Agreements

Information sharing agreements, sometimes known as 'Information sharing protocols' or 'data sharing protocols', set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have an information sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

An information sharing agreement must, at least, document the following:

- the purpose, or purposes, of the sharing;
- the legal basis for sharing under the DPA2018/UK GDPR;
- the legal basis to comply with the common law duty of confidence;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- who the data controller(s) is and any data processor(s)
- the data to be shared;
- data quality – accuracy, relevance, usability;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, other applicable GDPR rights, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- any particular obligations on all parties to the agreement, giving an assurance around the standards expected sanctions for failure to comply with the agreement or breaches by individual staff.

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

An information sharing agreement should be used the Trust, acting as data controller[8], is sharing information directly with other organisations that will act either as a joint data controller with the Trust, or as data controllers in their own right for that information.

Any processing by an organisation (e.g. supplier) on behalf of the Trust shall be governed by a data processing agreement, not an information sharing agreement. The UK GDPR requires a contract, or other legal act that is binding on the processor[9] with regard to the Trust as data controller, that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

Sharing for Non-care Purposes – There are requirements where confidential personal information needs to be shared for non-care purposes. Whether sharing with a "trusted organisation[10]" or not, the purposes for sharing need to be specifically documented and limited, and additional requirements such as recorded consent or evidence of support under Section 251 of the NHS Act 2006 may be required to enable lawful sharing.

In particular, when sharing information for 'non-care purposes' – often referred to as secondary uses (e.g. for purposes including commissioning, healthcare development, improving NHS resource efficiency etc.), the NHS Digital guidance 'A guide to confidentiality in health and social care' and the NHS Digital 'Secondary Use Services Guidance' (both referenced in section 11.2) both need to be complied with before any potential information is shared.

The Caldicott Report and subsequent 2013 Review recommends information sharing agreements should be developed between organisations sharing personal identifiable information.

Where it is decided that an Information Sharing Agreement needs to be documented a template is available from the Information Governance department.

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.

[8] 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'.

[9] 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.

[10] Trusted partner organisation. Refer to DSPT IR Guidance.

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.

For new technologies, you may be able to use a Data Protection Impact Assessment (DPIA) done by the product developer to inform your own Data Protection Impact Assessment (DPIA) on your implementation plans.

For new projects, Data Protection Impact Assessments (DPIA) is a vital part of Data Protection by design. They build in Data Protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented. No commitments to, or installation of systems, should take place before the DPIA has been signed off.

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. You need to keep it under review and reassess if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your Data Protection Impact Assessment (DPIA) assesses any new risks.

HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT

- Complete the screening questions[11] and send to the Information Governance team for review sfh-tr.information.governance@nhs.net. The Information Governance team will let you know the outcome of the screening questions.

- If after conducting a Data Protection Impact Assessment screening process, it appears that a Data Protection Impact Assessment is not required then the Data Protection Impact Assessment screening form will need to be completed and signed by the Information Asset Owner and Information Governance Lead.

- If the Information Governance team advise that a Data Protection Impact Assessment is required the DPIA template to be completed is available here[12]. Once completed you will need to send to the Information Governance team for review sfh-tr.information.governance@nhs.net.

[11] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8644
[12] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8644

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)**
IG toolkit validation	360 Assurance	Audit	Annually	IG Working Group/IG Manager/Audit and Assurance Committee/IG Committee
Adherence to IG policies and procedures in nominated Division	360 Assurance	Audit	Annually	IG Working Group/IG Manager/Audit and Assurance Committee/IG Committee
IAO report to the SIRO	IAO	Self-assessment return	Annually	IG Manager/SIRO/IG 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[13] 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.[14]

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
- Health and Social Care Act 2012 http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

[13] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[14] 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 Impact Assessment Screening Questions
- Data Protection, Confidentiality and Disclosures 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

Appendix 1	Equality Impact Assessment
Appendix 2	Guidance on the Law

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Information Sharing Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 23rd March 2023			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this policy	Already 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	None
Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None

Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None
What consultation with protected characteristic groups including patient groups have you carried out? •			
What data or information did you use in support of this EqIA? •			
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? • None.			
Level of impact Low Level of Impact			
Name of Responsible Person undertaking this assessment: Gina Robinson			
Signature:			
Date: 23rd March 2023			

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[15] 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.

[15] 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 Digital 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 Digital 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[16] 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.

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

The principle of Gillick competence[17] 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 s251 support.

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.

[17] 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[18]

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

[18] http://www.nwbh.nhs.uk/nhs-care-records-guarantee