Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

TRANSFER OF DATA POLICY

POLICY

Reference	IG 010		
Approving Body	Information Governance Committee		
Date Approved	21st September 2021		
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	September 2021		
Version	2		
Summary of Changes from Previous Version	Summarise changes if you are updating a current document. Not applicable to new documents		
Supersedes	1		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group Information Governance Committee		
Date of Completion of Equality Impact Assessment	27th August 2021		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Ensure compliance with: UK General Data Protection Regulation Regulation of Investigatory Powers Act 2000		
	The Telecommunications (Lawful Business Practice) Regulations 2000 Privacy and Electronic Communications Regulations		
Target Audience	All staff		
Review Date	2 years		
Sponsor (Position)	Chief Executive		
Author (Position & Name)	Information Governance Manager		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Governance Manager		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Not applicable	

CONTENTS

Item	Title	Page
1.0	INTRODUCTION	3
2.0	POLICY STATEMENT	3
3.0	DEFINITIONS/ ABBREVIATIONS	3
4.0	ROLES AND RESPONSIBILITIES	3
5.0	APPROVAL	5
6.0	DOCUMENT REQUIREMENTS	5
7.0	MONITORING COMPLIANCE AND EFFECTIVENESS	6
8.0	TRAINING AND IMPLEMENTATION	7
9.0	IMPACT ASSESSMENTS	7
10.0	EVIDENCE BASE (Relevant Legislation/ National Guidance) and RELATED SFHFT DOCUMENTS	7
11.0	KEYWORDS	7
12.0	APPENDICES	7

APPENDICIES

Appendix 1	EQUALITY IMPACT ASSESSMENT	8
Appendix 2	APPROVAL FOR TRANSFER OF DATA	10
Appendix 3	CHECKLIST AND SIGN OFF FORM FOR DATA TRANSFER	12
Appendix 4	THE CALDICOTT PRINCIPLES	15

1.0 INTRODUCTION

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

2.0 POLICY STATEMENT

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

3.0 DEFINITIONS/ ABBREVIATIONS

DTA - Data Transfer Agreement.
NHIS - Information Communication and Technology services are provided by Nottinghamshire Health Informatics Service, who are hosted by Sherwood Forest Hospitals NHS Foundation Trust.
Staff - All employees of Sherwood Forest Hospitals NHS Foundation Trust

4.0 ROLES AND RESPONSIBILITIES

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 Chief Financial Officer is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian
The Director of Corporate Affairs 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 Caldicott Guardian and works with the Senior Information Risk Owner and 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 considers the nature, scope, context, and purposes of processing.

Information Asset Owners (IAOs)
Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)
Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents, and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

All Staff
All Trust employees and anyone else working for The Trust (e.g. agency staff, honorary staff, management consultants etc.) who use and have access to Trust personal information must understand their responsibilities for Data Protection and confidentiality.

5.0 APPROVAL

Policy approval is by the Information Governance Committee.

6.0 DOCUMENT REQUIREMENTS

6.1 TRANSFER OF DATA OWNERSHIP

If there is an intention for data ownership to be transferred to another organisation, reasonable notice must be given to NHIS by the receiving or transferring organisation.

All intentions to transfer ownership of data from and to another organisation must be documented on the form found at Appendix 1. This form must be accompanied by a covering letter authorised by the organisational Information Governance Lead (or Data Protection Officer) within the provider and receiver of the data.

Before any data is transferred, the transferring organisation must state exactly what data is to be transferred. It will be the responsibility of the transferring organisation to collate and document all information and data sets which are the subject of transfer (see Appendix 1).

Should data be required to transfer between legal organisations a Data Transfer Agreement (DTA) will be required. The receiving and transferring organisations are responsible for ensuring that legal advice is undertaken in relation to the data transfer agreement and this advice should be sought prior to any data being transferred.

The data transfer agreement must detail the data to be transferred and include all data sets which are to be transferred to the subsequent organisations, as a specific authorised instruction to NHIS prior to any action being taken.

6.2 TRANSFER OF DATA TO NHS DIGITAL

Secure Electronic File Transfer (SEFT)

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

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

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (e.g. verbal, formal report etc) and by who)
All requests for the transfer of data ownership from the customer to a subsequent organisation will be logged into the call management software in use at NHIS and given a unique reference number and monitored with reference to the SLA.	NHIS Head of Governance and Assurance and Information Governance Manager	Audit	Annual	Information Governance Working Group

8.0 TRAINING AND IMPLEMENTATION

It is a Line Management responsibility to ensure that all staff are trained on the application of the policy. The policy will be circulated to all staff and made available on the intranet.

9.0 IMPACT ASSESSMENTS

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

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

Evidence Base:

- Data Protection Act 2018
- National Cyber Security Centre Guidance

Related SFHFT Documents:

- Information Security Policy
- Data Protection, Confidentiality and Disclosure Policy
- Safe Haven Procedure

11.0 KEYWORDS

Information, Data Protection, Archive, Backup.

12.0 APPENDICES

Refer to list in contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Data Transfer Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 27th August 2021			
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?

- Information Governance Working Group
- Information Governance Committee

What data or information did you use in support of this EqIA?

- Trust guidance for completion of the Equality Impact Assessments

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: G. H. Robinson

Date: 27th August 2021

APPENDIX 2 – APPROVAL FOR TRANSFER OF DATA

Transferring Organisation:	
Service/Directorate Name:	
Completed By (Lead Contact):	
Job Title:	
Receiving Organisation:	
Receiving Org Contact Details:	
Completed By (Lead Contact):	
Job Title:	
Date:	

Section 1 - Key Information

1. Describe the information held and the purpose of the data or service: Please include as much detail as possible, including the file path and names of all the folders and sub folders	
2. Proposed date to enable transfer:	
3. Other supporting information which forms part of this application: for example type of data; is this person identifiable data	
4. New location of the data and how it will be transferred and stored:	

Section 2 – Sign Off

User Agreement

I the undersigned agree the transfer is appropriate and in accordance with organisational information governance policies and procedures.

I have read and understood the organisations Information Security Policy, Data Protection, Confidentiality and Disclosure[1], and I understand the implications as outlined by the organisation of the Computer Misuse Act, and Data Protection legislation in processing of data. In line with national guidance and the organisations' policy I will not process any person identifiable information on non-organisational equipment.

I agree that any data processing that I undertake will be carried out in line with Data Protection legislation. I understand that any breach of these conditions will result in disciplinary processes.

Transferring Organisation:	
Signed:	**Date:**
Receiving Organisation:	
Signed:	**Date:**
Information Asset Owner	
Signed:	**Date:**
Name:	
Job Title:	
Contact Number:	
IT Use Only	
Date Access Given:	
Name:	
Signature:	

[1] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

APPENDIX 3 – CHECKLIST AND SIGN OFF FORM FOR DATA TRANSFER

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

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

A Data Controller should explicitly state what is expected from its Data Processors and this should be achieved through formal contracts (rather than Service Level Agreements) even when between NHS organisations. The contracts should create clarity about the services and provide mutual protection given the liabilities that each are under in delivering services. There will be legal terms of transfer between Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) services that are transferring and the relevant receiving organisation – the transfer of records should be included as part of the formal transfer of assets, alongside premises, staff, and hardware.

If the receiving organisation does not want to take the archived or historical data, then responsibility for the data's continued existence must be clarified at the point of transfer; for example what the continuing arrangements are for further storage and retention of the documents.

Information sharing protocols and confidentiality agreements will need to be set up where multiple providers use single instances of software to support patient care across organisations.

The following considerations provide a checklist for determining what arrangements need to be in place for the data transfer.

CONSIDERATIONS

Q1. Are the organisations to which records and data (and responsible for it as Data Controller) being transferred to existing legal entities?
Q2. Are the datasets included in the formal statements on transfer of assets between organisations? There may be issues on timing about this, but reference to the need to transfer datasets and records should be made in the formal statements with details clearly stated subsequently in related formal schedules.

Q3. Which organisation owns the system in terms of hardware and software and relevant licences? – this organisation is the System Owner. The System Owner for data from transferred provider arms may, for example, be a Trust or community service provider
Q4. Which organisation(s) determines the purposes for which the personal data in the system are used (e.g. what data is held on and what reports and analyses are required to check what is happening to Mrs Smith)? – this organisation is the Data Controller (which may also be the System Owner); there may be more than one Data Controller acting jointly.
Q5. Which organisation is responsible for safeguarding and processing the data? This organisation is the Data Processor (which may also be the Data Controller).
Q6. Have Data Protection Impact Assessments been undertaken for records, data and systems been undertaken? In particular, have DPIAs been undertaken in relation to sensitive services?
Q7. If different organisations are identified in Q1, Q2 and Q3, then are there suitable statements and service level agreements between the organisations to define roles etc?
Q8. Have the receiving organisations notified the Information Commissioners Office (ICO) of changes to their data controller and data processing responsibilities?
Q9. Are any data 'orphaned' as a result of the data transfer? If yes, are there appropriate data processing and retention agreements in place?
Q10. If data and information are shared between organisations or accessed across organisations, are relevant Information Sharing Protocols or Acceptable Use Policies and staff confidentiality agreements in place? Where necessary are these supported by Subject Specific Information Sharing Agreements?

Q11 Where there is orphaned data and information-sharing protocols are in place, have checks been made that inadvertent unauthorised access cannot be made to orphaned data or to records for patients for whom the service provider does not have responsibility? If such access can be made, relevant remedial steps are required.
Q12. If a system external to the NHS is to be used to process health sourced personal data, are there appropriate safeguards on data access in place? If not, has explicit consent for the wider use of the data been obtained from the Data Subjects?
Q13. Does the system fully support Data Protection Act 2018 requirements, Caldicott Principles, and the Confidentiality: NHS Code of Practice? In particular, can user access be restricted to only that data that the user should see, either on the basis of organisational responsibility or their care service provision responsibility (role-based access provisions)?
Q14. If the answer to Q13 is no, then are steps being taken to offset potential inappropriate data access – e.g. only nominated and authorised staff can access health records and vice versa?
Q15. Are relevant Registration Authority (smartcard) and user registration mechanisms in place?
Q16. Can the receiving organisation meet the DPA 2018 requirements of Subject Access requests?
Q17. Have patients or service users been informed that their data has been transferred and (where appropriate) that additional staff may now access their records? Have privacy notices been modified to reflect induced changes?
Q18. Have the organisation's Information Governance policies and procedures been created/amended to reflect the new responsibilities resulting from implementing?
Q19. Is additional Information Governance or security training required for staff as part of implementation?

APPENDIX 4 – THE CALDICOTT PRINCIPLES

Principle 1 - Justify the purpose for using confidential information
This means you should not use or share information unless you have a valid reason.

For example, wanting to send a friend a birthday card is not a valid reason to access the records your organisation holds about them.

Principle 2 – Do not use the confidential information unless it is absolutely necessary
If you believe you have a valid reason, ask yourself if it is essential that you use confidential information, or can the purpose be met without identifying any individual?

For example, if you are asked for information about how many people have attended for an appointment, it would not be necessary to provide the names and addresses of each person who attended.

Principle 3 - Use the minimum necessary confidential information
If you must use confidential information, you need to be clear on what is required to meet the purpose. If a particular part of the information is not necessary, it should not be used or shared.

For example, if you receive a valid request for details about a patient/service user's last attendance at your organisation, it would not be appropriate to provide the requestor with the entire record or care/treatment.

Principle 4 - Access to confidential information should be on a strict need-to-know basis
Information should only be available to authorised members of staff. You should not attempt to access information that you do not need to see as part of your role or use someone else's account details.

You should never allow anyone to log into systems using your details. If you intend to share the information, it should only be shared with those who need it to carry out their role.

Principle 5 - Everyone with access to confidential information should be aware of their responsibilities
You should attend the provided training and awareness session so that you understand your responsibilities for protecting information.
If you intend to share the information, you must ensure that the recipient is aware of their responsibility for protecting the information and of the restrictions on sharing it further.

Principle 6 - Understand **and comply with the law**
When you use confidential information, there is a range of legal obligations for you to consider. The key obligations are outlined in the Common Law Duty of Confidentiality and under the UK General Data Protection Regulation.

If you have a query about the disclosure of confidential information, you should contact your line manager, then the Information Governance lead (or equivalent) if you are still not sure.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality.
You should have the confidence to share information in the best interests of your patients and service users within the framework set out by these principles.

Principle 8: Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information - in some cases, greater engagement will be required.