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	28th November 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	December 2023		
Version	3		
Summary of Changes from Previous Version	Data transfer agreement template added		
Supersedes	2		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group Information Governance Committee		
Date of Completion of Equality Impact Assessment	24th July 2023		
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 Network and Information Systems Regulations 2018 (UK)		
Target Audience	All staff		
Review Date	2 years		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Head of Data Security and Privacy, Jacquie Widdowson		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Head of Data Security and Privacy		

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

CONTENTS

APPENDICIES

1.0 INTRODUCTION

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

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

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

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

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

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

2.0 POLICY STATEMENT

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

3.0 DEFINITIONS/ ABBREVIATIONS

Data Controller	The Trust is registered as a Data Controller with the Information Commissioner's Office. A Data Controller is defined as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed'.

Data Processor	A processor is a natural or legal person (not an employee) public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.
Data Transfer Agreement	A data transfer agreement (DTA) is a legal document that lays out the terms and conditions of sending or receiving personal data to another jurisdiction or organisation. This agreement will include provisions for how data will be used and protected as a result of the transfer.
ICO (Information Commissioner's Office)	The ICO is the supervisory authority for data protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance, and take enforcement action where appropriate.
Personal data	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 i.e. 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.
Processing	Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.
Special categories of	The special categories of personal data are: a) racial or ethnic origin

personal information (or data)	b) political opinions c) religious or philosophical beliefs d) trade-union membership e) genetic data f) biometric data for the purpose of uniquely identifying a natural person g) data concerning health h) data concerning a natural person's sex life or sexual orientation

4.0 ROLES AND RESPONSIBILITIES

Trust Board

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

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 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 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 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 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

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Article 24(1) of the UK GDPR says that:

- we must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR.
- the measures should be risk-based and proportionate; and
- we need to review and update the measures, as necessary.

Contracts must include certain specific terms as a minimum, such as requiring the processor to act appropriately to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the UK GDPR.

Similarly, if a processor uses another organisation (i.e. a sub-processor) to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor.

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.

Contracts must set 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 subject; and

- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions.
- the duty of confidence.
- appropriate security measures.
- using sub-processors.
- data subjects' rights.
- assisting the controller.
- **end-of-contract provisions**; and
- audits and inspections.

Being responsible for compliance with the UK GDPR means that we need to be proactive and organised about our approach to data protection.

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 data.

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.

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 3.

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 3).

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 from the Information Governance team.

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. Appendix 3 should be completed and forwarded to IG and Digital Business Team for review prior to any action being taken.

Legal obligations which mandate continued access to data following cessation of contract (for example where care provision has moved from one provider to another) must be clearly stated at the commencement of the contractual relationship and noted that data controller responsibilities will be maintained for records generated and where there is an ongoing potential for litigation against the provider of care for the time of the contract period.

6.2 TRANSFER OF DATA TO NHS ENGLAND

Secure Electronic File Transfer (SEFT)

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

SEFT can only be accessed by registered and approved users. NHS 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.

6.3 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A DPIA is a legal requirement and must be conducted prior to the transfer of data, this will help minimise any data protection risks that could result to individuals. A DPIA supports and ensures any privacy risks are mitigated to an appropriate level and that the transfer of data is completed in a secure manner.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

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

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: 24th July 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?

- 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: 24th July 2023

APPENDIX 2 – CHECKLIST FORM FOR DATA TRANSFER

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 registered with the ICO as a data controller? Check the register here
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 3 – DATA TRANSFER AGREEMENT

Start date		
The Parties	**Exporter**	**Importer**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Importer Data Subject Contact		Job Title: Contact details including email:
Signatures confirming each Party agrees to be bound by this DTA		

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 Policy, 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.

Signed for and on behalf of the Exporter.

	Name	Job Title	Date
Information Asset Owner			
Data Protection Officer			
Senior Information Risk Owner			
Caldicott Guardian			
Chief Digital Information Officer			
Patient safety[1]			
NHIS			

Signed for and on behalf of the Importer.

	Name	Job Title	Date
Information Asset Owner			
Data Protection Officer			
Senior Information Risk Owner			
Caldicott Guardian			
Chief Digital Information Officer			
Patient safety[2]			
NHIS			

[1] DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital
[2] DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital

Table 2: Transfer Details

UK country's law that governs the DTA:	☐ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☐ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☐ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☐ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third-Party Controller)
Whether UK GDPR applies to the Importer	☐ UK GDPR applies to the Importer's Processing of the Transferred Data ☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: Date of agreement: Parties to the agreement: Reference (if any): **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: Date of agreement:

	Parties to the agreement: Reference (if any): **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: Date of agreement: Parties to the agreement: Reference (if any):
Term	The Importer may Process the Transferred Data for the following time period: ☐ the period for which the Linked Agreement is in force ☐ time period: ☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Can the Importer make further transfers of the Transferred Data?	☐ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section **Error! Reference source not found.** (Transferring on the Transferred Data). ☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section **Error! Reference source not found.** (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section **Error! Reference source not found.**: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☐ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: ☐ each month(s) ☐ each quarter

	☐ each 6 months ☐ each year ☐ each _____ year(s) ☐ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Personal Data	The Transferred Data includes data relating to: a name an identification number i.e. NHS number, NI number location data an online identifier i.e. 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
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of uniquely identifying a natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☐ none of the above
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ☐ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section **Error! Reference source not found.**.
Purpose	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 The Importer may Process the Transferred Data for the following purposes: ☐ The Importer may Process the Transferred Data for the purposes set out in: In both cases, any other purposes which are compatible with the purposes set out above. ☐ The purposes will update automatically if the information is updated in the Linked Agreement referred to. ☐ The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section **Error! Reference source not found.**.

Table 4: Security Requirements

Security of Transmission	
Security of Storage	
Security of Processing	
Organisational security measures	
Technical security minimum requirements	
Updates to the Security Requirements	☐ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☐ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section **Error! Reference source not found.**.

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.