NHS
Stockport
NHS Foundation Trust

INFORMATION SHARING & TRANSFER OF RECORDS POLICY

CONTENTS

EXECUTIVE SUMMARY

This document and associated policies and procedures identify the principles required to ensure that all staff comply with the law and best practice when handling information and to ensure that information is shared in an appropriate manner and secured in transit.

All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation.

Where departments within the Trust, other NHS Trusts or other agencies want to send personal information to a Trust department, they should be confident that they are being sent to a location which ensures the security of the data.

The details of every NHS Trust's safe haven point are listed in the National Safe Haven Directory.

A number of Acts and guidance dictates the need for safe haven arrangements to be set in place, they include:

Data Protection Act 2018 (Principle 6): "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

United Kingdom - General Data Protection Regulation (UK-GDPR) (Article 5 1(f) 'Integrity and Confidentiality'): As per principle 6 above.

Confidentiality: NHS Code of Practice 2003: Annex A1 Protect Patient Information *"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be"*

Further information can be found on the **Information Governance and Security** microsite on the Trust Intranet, which has up-to-date polices, guidance and codes of practice. Detailed procedures for each method of transfer are available on this site. This policy should be read in conjunction with these procedures.

Director of Informatics

SCOPE AND PURPOSE

This policy applies to Stockport NHS Foundation Trust, referred to as the 'Trust', and includes all hospitals, units and community health services managed by Stockport NHS Foundation Trust.

This policy provides:

- The legislation and guidance which dictates the need for a safe haven.
- A definition of the term safe haven.
- When a safe haven is required.
- The necessary procedures and requirements that are needed to implement a safe haven.
- Rules for different kinds of safe haven.

The processes described in this policy must be followed by all Trust staff, unless exceptional circumstances arise, which may have an impact on direct patient care and when advice/guidance has been sought.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate.

This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

ROLES AND RESPONSIBILITIES

Senior Information Risk Owner (SIRO)

The Trust’s Chief Finance Officer is the Trust’s Senior Information Risk Owner and has responsibility for ensuring information risk is appropriately managed across the Trust on behalf of the Trust Board of Directors.

Caldicott Guardian

The Caldicott Guardian is the Trust’s Medical Director**.** The Caldicott Guardian has responsibility for safeguarding the confidentiality of patient information.

Information Governance Team

The Information Governance Team is responsible for coordinating improvements in data protection, confidentiality and information security.

Informatics Department

This is the official designated safe haven location in Stockport NHS Foundation Trust, the Informatics team will ensure that appropriate safe haven processes are in place. For secondary use, the information team will ensure that any queries and reports produced will be effectively anonymised, where appropriate, and suitably encrypted when anonymisation is not possible.

All Trust Managers:

Managers within the Trust are responsible for ensuring that the policy, and other associated policies and supporting standards and guidelines are built into local processes and that there is on-going compliance.

Managers are accountable for the communication about and compliance with Trust policies, and must ensure that staff are adequately trained and apply the appropriate guidelines.

All Trust Staff:

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff is responsible for any records or data they create and what they do with information they use.

Staff should ensure they attend information governance training and awareness sessions to maintain their knowledge and skills.

All staff has a responsibility to adhere to information governance standards which are written into the terms and conditions of their contracts of employment.

All staff that process personal-identifiable information and managers who have responsibilities for those staff must ensure that they abide by this policy.

GLOSSARY OF TERMS

Safe Haven:

The term safe haven is a location situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely. In a Trust they are the point from where person identifiable data is controlled.

The official designated safe haven location in Stockport NHS Foundation Trust is:

Stockport NHS Foundation Trust
Room 19, Informatics Department

2nd Floor, Cedar House
Stepping Hill Hospital
Poplar Grove, Stockport
SK2 7JE

Tel: 0161 419 4317

All staff should be aware of this location, especially as some calls and mail are directed to the listed safe haven only.

However, any department sending, receiving, holding or communicating person identifiable data, concerning either patients or staff, should provide safe haven conditions by following the guidelines set out within this policy.

Person Identifiable Information / Data (PID):

This is also referred to as, "personal / confidential information" and relates to information about a person which would enable that person's identity to be established by one means or another.

This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified.

All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. This includes the nationally recognised NHS number.

Sensitive Information:

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community.

This is wider than, but includes, data defined as special category under the Data Protection Act 2018.

In addition to personal and clinical information, financial and security information is also likely to be deemed "sensitive".

Examples of sensitive information include information in relation to a person's:

- Health or physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Trade Union membership
- Biometric

- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

Primary and Secondary uses of Information

Primary Use (Direct Care) – is when information is used for direct healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

Secondary Use (Non-Direct Care) – is when information is not used for direct healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. PID should not be used for secondary use purposes so any data shared **must be** limited and de-identified using anonymisation or pseudonymisation techniques.

Anonymised or Pseudonymised Information

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity.

- **Anonymisation** - requires the removal of name, address, full postcode, NHS Number and any other detail or combination of details that might support identification.

- **Pseudonymisation** **-** requires replacing person identifiers in a dataset with other unique values (pseudonyms) from which identities of individuals cannot be inferred, e.g. the replacement of an NHS number with another random number. Pseudonymisation may be reversible or irreversible

Mobile Devices or Removable Media:

This includes laptops & tablets, smartphones, portable hard drives, DVD & CD-ROM, solid state memory cards, USB memory sticks.

Information / Data Flow / Information Flow Mapping

This is the process of documenting the flow of information from one physical location to another and the method by which it "flows". Data flows may be by: Verbal transfer, e-mail, text, instant messaging, post/courier, portable electronic or removable media.

Information Sharing Agreement

An Information Sharing Agreement should be used when sharing personal data with Health and Social Care Organisations and other partner agencies. It sets out general principles with which both parties must comply at all times. It specifies the categories of data that will be shared and the purpose(s) for which the recipient is permitted to use each category of data, including specific security measures that the parties shall put in place to protect the data. It must be signed by the Caldicott Guardian or authorised senior officer of each organisation.

Confidentiality Agreement / Data Processing Agreement

A confidentiality agreement may be used by third party contractors providing services, including support, maintenance or consultancy where they may have access to person identifiable or sensitive data on-site, or off-site (including via remote access).
A data processing agreement or contract should be used by third party suppliers that provide information systems or services for processing of data, including hosted and managed services.

Data Protection Impact Assessment (DPIA)

When undertaking any data sharing initiatives or projects that involve the processing of personal data, a data protection impact assessment (DPIA) should be undertaken in conjunction with the Information Governance Team to ensure compliance with the Data Protection Act and UK GDPR.

THE PROCESS

Requirements for Safe Havens

A Safe Haven is defined as a safe and secure mechanism to ensure person-identifiable information can be held, received and communicated securely. The term relates to physical locations, equipment (such as printers) or the process by which information is transported. This section deals with how Safe Havens operate as part of the day to day handling of person-identifiable information.

Location/Security Arrangements:

- Any department or any person sending/receiving person identifiable information should consider the physical security arrangements i.e. a room that is locked or preferably accessible via a coded key pad known only to authorised staff, this key pad should be in use at all times. This should be the first step in the aim to create safe haven conditions.

- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.

- If sited on the ground floor, any windows should have locks on them.

- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.

- Manual paper records containing person-identifiable information should be stored in locked cabinets, where possible.

- Computers should not be left on view or accessible to unauthorised staff and the screen ‘locked’ (using Ctrl, Alt, and Delete keys simultaneously / windows and ‘L’ key) or be logged/switched off when not in use.

- Equipment such as printers in the safe haven should have a coded password and be turned off out of office hours.

- Confidential information should not be removed from a safe haven office unless absolutely necessary.

- Operate a clear desk policy, especially when hot desking or working in an open plan office.

Communication by Post:

- All sensitive records must be placed face down in public areas and not left unsupervised at any time.

- Incoming mail should be opened away from public areas.

- Outgoing mail (both internal and external) should be sealed securely in robust envelopes and marked ‘private and confidential’ or ‘private and confidential - to be opened by addressee only’ (if the information is particularly sensitive or intended for a particular individual). Where possible use tamper-evident envelopes or tape/seals.

- Where sending bulk personal/sensitive information – such as a medical record - use recorded/registered delivery or secure courier services. This is not necessary when sending single sheets such as appointment letters, however care must be taken to ensure that only the name and address is visible and that no personal information can be viewed through any window envelopes.

- Confirm the name, department and full address of the recipient before sending any information out, and ask the recipient to confirm receipt.

- Ensure information is sent to a safe location.

- Under no circumstances should patient information be sent in the internal mail, across the Stepping Hill site. For staff who need to transport information from site to site (in particular staff working in the community), it is acceptable to transport via the internal mail however such staff will be responsible for ensuring:

(a) The information is transported in a secure/robust, adequately sealed envelope, and

(b) Accurate tracking information is recorded (to include the date the information is put into the postal system; the location of the pick-up point i.e. where the outgoing post- tray is located; the name, address and job-title of the recipient

(c) Recipients contact the sender to confirm receipt, to allow the tracking information to be updated

Computers:

- Access to any PC or laptop must be password protected; passwords must not be shared, written down or disclosed in any way.

- Computer screens must not be left on view so members of the general public or staff, who do not have a justified need to view the information, **cannot** see personal data.

- PCs or laptops not in use should be logged/switched off or the screen 'locked' (using Ctrl, Alt, and Delete keys / windows and 'L' key) when not in use.

- Information should be held on the Trust's network drives, for example 'I' drive, 'J' drive or 'S' drive and **not** stored on local computer hard drives i.e. 'C' drive (usually 'my documents'). Departments should be aware of the high risk of storing information locally and take appropriate security measures e.g. Encryption and Back-Up Procedures.

- Confidential Information stored on network shared drives should be restricted as appropriate to authorised users. IT services can assist in establishing folder access rights.

- Undertake regular house-keeping of your files, ensuring only the minimum amount of data is retained, in accordance with the Trust's Records Management Policy and NHS Records Management Code of Practice Retention Schedules.

- The Information Governance Team must be informed of any new database/system or applications created/introduced that contain person identifiable information.

- Any database system or application, containing personal information should comply with the Data Protection Act Principles and the Caldicott Principles with appropriate security measures. A DPIA may have to be undertaken.

E-mail:

Great care should be taken in sending personal information, especially where the information may be of a clinical nature – it should be secure (encrypted) and procedures undertaken to ensure that the correct person has received it.

Email should only be used to send person identifiable information if absolutely necessary, appropriately authorised and encrypted to the appropriate standard.

The Trust email (@Stockport.nhs.uk) is accredited to the secure email standard DCB 1596, which is to the same standard as NHS mail (@NHS.net), so you can securely email to the following secure email domains:-

NHS:

NHS.net

NHS.uk (Only if those NHS organisations that have obtained accreditation to the secure email standard from NHS Digital and have been whitelisted (published on NHS digital website https://digital.nhs.uk/services/nhsmail/the-secure-email-standard) as a secure email domain)

Local Government:

Gov.uk

Central Government:

Cjsm.net

Pnn.police.uk

Mod.uk

Parliament.uk

The email address must contain one of the domains above IN FULL

Otherwise, if sending to other non-secure email domains it is important to continue to comply with the following:

- All personal information sent by e-mail should be encrypted to NHS cryptographic standards (currently 256bit strength). The Trust local email has an email encryption facility (Trend Micro) that can be used to send information securely (encrypted)
  Encryption must be applied manually by typing **[secure]** (including the square brackets) in the subject header of the e-mail message. Further guidance can be found on the IG & Security microsite.

- Emails are sent to the right people. Confirm the intended email address before sending and ask the addressee to acknowledge receipt.

- The receiver is ready to handle the information in the right way.

- Clinical information should be clearly marked.

- Person identifiable information should not be written in the ‘subject’ box and messages should be anonymised wherever possible i.e. the use of a reference rather than individual names.

- Browsers are safely set up so that, for example, passwords are not saved and temporary internet and e-mail files are deleted on exit.

- Information sent by email will be safely stored and archived as well as being incorporated into patient records.
- There is an audit trail to show who did what and when.
- There are adequate fall back and fail-safe arrangements.
- Information is not saved or copied into any PC or media that is “outside the NHS” such as personal devices. Any information should be stored on the Trust network.
- Emails no longer required should be archived/deleted from the system (Ref: NHS Records Management Code of Practice – Retention Schedules).

There are occasions when patients ask to correspond with the Trust via e-mail. This is not the Trust’s preferred method and patients must be advised that any correspondence conducted via unencrypted e-mail is not secure. The Trust does have an encryption facility which can be used when sharing information via e-mail and patients should be encouraged to use this method. However, if a patient is not happy to use our encryption facility, preferring to use their own e-mail address, we must reiterate to them that the information is not secure and that the Trust cannot be responsible for the safe delivery of their data. As long as the patient confirms an understanding of this fact and accepts responsibility for continuing to use unsecured e-mail, and such acceptance (in writing) is recorded in the patient notes, it may be acceptable to use this method of corresponding with the patient.

Seek advice from the Information Governance Team or IT services, with regards to encryption solutions, secure erasing methods, or restricted access rights to shared drives.

Please also read the Stockport NHS Foundation Trust IT Acceptable Use Policy for more guidance.

Phone:

- Information should not usually be provided over the telephone as the identity of the caller cannot always be verified.
- Always confirm the name, job title, department, and organisation of the person requesting the information.
- Confirm the reason for the information request.
- Take a contact number i.e. main switchboard (never a direct line or mobile telephone number).
- Call them back (always call the switchboard) to confirm the details, if necessary.
- Check whether the information can be provided; if in doubt tell the enquirer that you will call them back.

- Only provide information to the person who requested it, do not leave messages.

- Ensure that you record details of the information disclosed, your name, date and time of disclosure, the reason for the disclosure, and who authorised the disclosure. Also record the recipient's name, job title, organisation and telephone number.

- Ensure that you have a password protected voice mail in operation for any messages that you might receive.

Other Transportation Arrangements:

- Person identifiable information, including paper records, should only be taken off site when absolutely necessary and appropriately authorised, e.g. for community nursing staff, secure document carriers should be used at all times. Best practice would be to use secure wallets available from Supplies.
  In any event, information MUST be transported in a sealed container (such as briefcase) and must not be transported 'loose' such as in a folder.
  This includes attendance at Coroners Inquests. It is not permitted, in accordance with the 'Procedure for Preparing for And Attending an Inquest', to transport the full Inquest pack to the Inquest. Staff should carry with them the original hospital records required for their evidence and their own statement.

- Where information is required (and appropriate) to be transported off site, in these circumstances, sensitive information should be transported out of sight (in a car boot); should never be left unattended and should NEVER be left in the car overnight. If information cannot be returned to base at the end of a shift, it should be removed from the car and stored overnight in the member of staff's house/apartment.

- A record of what information you are taking off-site should always be documented, including why, where and to whom you are taking it.

- Paper records must be transported in a sealed/secure container.

- Never leave person identifiable information unattended.

- Ensure that all information is returned back to the site as soon as possible, and that any records are updated.

- Where information is required in electronic format to be taken offsite, only trust issued mobile devices or removable media should be used, which should be appropriately encrypted. The information must not be transferred to personal home computers or mobile devices.

- Personal data should not be sent outside of the UK without seeking advice from the Information Governance Team.

Displaying Personal Information (for example on white-boards)

Boards containing patient information / person identifiable information should ideally be sited in areas that are **not** generally accessible by the public, e.g. staff offices. These rooms should be clearly marked 'staff only' and windows obscured appropriately.

With regard to patient identifiable information recorded on Ward Whiteboards, it is Trust policy that only initials are used (the exceptions are where there are two patients with the same surname when an initial can be used **by exception**, ED and Paediatrics who may use a first name and an age). This requirement relates also to the smaller side-room Whiteboards but does not apply to whiteboards above a patient's bed when the full name can be used.

If it is absolutely necessary (and this must be by exception) to put clinical information onto a whiteboard, the information must be abbreviated or symbolised so that only health professionals can understand the information and no other members of staff (or other patients/patient relatives) that may come into the department.

The use of personal information in patient areas should be carefully considered and a risk assessment undertaken by an appropriate manager.

Sharing Information with other Organisations

Person Identifiable Information must only be shared if:

- You have patient consent or
- If a law says you have to or
- It's in the public interest

Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek assurance that these organisations have a designated safe haven point for receiving personal information.

The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 2018.
- Common Law Duty of Confidence.
- Confidentiality: NHS Code of Practice 2003.

This assurance will be obtained by completing a Data Protection Impact Assessment document. This is a legal requirement under the Data Protection Act 2018. Copies of the template, together with advice and guidance can be obtained from the Information Governance Team.

An information sharing agreement must be put in place with NHS and local government information sharing partners and organisations where personal information is to be shared.

A confidentiality agreement or data processing agreement should be used with commercial third party suppliers of information systems and services, including support, maintenance or consultancy where the third party may have remote access or access to person identifiable or sensitive data on-site, or off-site.

Once the appropriate agreements have been signed and approved, any access to Trust systems can only be granted on completion of the Trust Request for External Access Form/Personal Confidentiality Agreement Form. This form must be signed by the applicant; a senior clinical officer (to assure us that the request is appropriate and that the relevant legal justification for providing access is sound). The form can be obtained from the Information Governance team and then must then be returned to the Information Governance via (externaluser@stockport.nhs.uk) who will then arrange to have the form counter-signed by the Trust's Clinical Medical Director (or the Deputy Medical Director), as required. Arrangements will then be made with IT once the form has been appropriately authorised and counter-signed.

All flows of information coming in and going out of the department should be risk assessed as appropriate, and this is managed via the Data Protection Impact Assessment documentation. Advice should be sought from the Information Governance Team, as required.

Sharing Information Internally with 3rd Parties

There will be occasions where you may have to work with people employed by an external 3rd party on Trust premises, on the Trust's behalf, e.g. external consultants or contractors. The Data Protection principles and the guidance around duty of confidentiality still apply. Unless it is for the purpose of providing **direct healthcare**, no person identifiable information can be shared. Any identifiers must be removed before the information is shared and any sharing must be done in a secure manner.
A confidentiality agreement should be in place with the third party employee.

Anonymisation process

The Trust has adopted a policy of anonymisation rather than pseudonymisation, which would involve specialist software products.

The overall aims of anonymisation are to enable:

- The legal and secure use of patient data for secondary purposes by the NHS and other organisations involved in the commissioning and provision of NHS-commissioned care.

- NHS business is not using identifiable data in its non-direct care related work wherever possible.

All regular reports and ad-hoc requests for patient or activity level data will have all patient identifiable data removed and therefore be effectively anonymised.

Secure File Transfer

Other methods of secure file transfer and uploading of data may be considered but advice should be sought from the IG team to ensure a secure process.

Further information and guidance is available on the Information Governance & Security Microsite or by contacting the IG Department directly.

TRAINING

Staff should undertake annual data security awareness training to maintain their knowledge and skills.

MONITORING COMPLIANCE

The Trust is committed to ensuring compliance with documents and will actively monitor the effectiveness of such documents.

The Trust will regularly monitor and audit its Safe Haven & Information Sharing practices for compliance with this policy.

The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the policy is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Information Governance & Security Group, Digital and Informatics Group and the Audit Committee, as appropriate.

Process for monitoring compliance with this policy

CQC Regulated Activities	Process for monitoring e.g. audit	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/group / committee for review of results	Responsible individual/group/ committee for development of action plan	Responsible individual/group/ committee for monitoring action plan and implementation
	Internal Audit Data Security and Protection Toolkit External Audit	Information Governance & Security Group	Annually	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group

DOCUMENT LAUNCH AND DISSEMINATION

Launch

The responsibility of implementing this document, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff (including agency staff) to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

This document has been compiled by the Information Governance Team in consultation with Governance Leads for each Division by means of the Information Governance & Security Group.

Once finalised, the document will be presented to the Digital and Informatics Group. The document will then be displayed on the Information Governance & Security microsite on the Trust's intranet and on the Trust's website. Managers and Governance leads should ensure the information is cascaded to all staff.

Dissemination

Information Governance & Security Microsite
Trust Website

REFERENCES AND ASSOCIATED DOCUMENTATION

Information Governance Policy
Information Security Policy
Information Security Incident Reporting/Management
IT Acceptable Use Policy

Mobile Devices & Removable Media Security Policy
Agile and Homeworking Policy
Photography/Video & Audio Records of Patients/Staff
Network Security Policy
Data Protection & Confidentiality Policy
Access to Personal Information (Subject Access) Policy
Data Quality Policy
Freedom of Information Policy
Information Lifecycle & Records Management Policy
Disciplinary Policy
Incident Reporting SOP
Inquest Policy

EQUALITY IMPACT ASSESSMENT

Office Use Only

Submission Date:	12/02/2020
Approved By:	*Annela Hussain*
Full EIA needed:	No

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the Policy/SOP/Service**	Information Sharing & Transfer of Records Policy	
2	**Department/Division**	Information Governance – IM&T	
3	**Details of the Person responsible for the EIA**	**Name:**	Joan Carr
		Job Title:	IG Co-ordinator
		Contact Details:	Information.governance@stockport.nhs.uk
4	**What are the main aims and objectives of the Policy/SOP/Service?**	To provide guidance for staff in order to maintain and uphold the Trusts information governance requirements	

For the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a <u>differential</u> impact on any of the protected characteristics below? Please state whether it is positive or negative. What data do you have to evidence this?** **Consider:**	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward

	What does existing evidence show? E.g. consultations, demographic data, questionnaires, equality monitoring data, analysis of complaints. Are all people from the protected characteristics equally accessing the service?	e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Produce action plan if further data/evidence needed ✓ Re-visit after the designated time period to check for improvement.	Lead
Age	No differential impact		
Carers	Positive Impact		
Disability	Positive Impact		
Race / Ethnicity	Positive Impact		
Gender	No differential impact		
Gender Reassignment	Positive Impact		
Marriage & Civil Partnership	No differential impact		
Pregnancy & Maternity	Positive Impact		
Religion & Belief	Positive Impact		
Sexual Orientation	Positive Impact		
General Comments across all equality strands	This policy is likely to have a positive impact across some protected characteristics: In addition to personal and clinical information, financial and security information is also likely to be deemed "sensitive" (see page 7). For this type of information even more stringent measures should be employed to ensure that the data remains secure. Trust wide documents can be made available in a number of different formats and languages if requested.		

Action Plan

What actions have been identified to ensure equal access and fairness for all?

Action	Lead	Timescales	Review & Comments

EIA Sign-Off	Your completed EIA should be sent to Equality, Diversity & Inclusion Manager for approval: equality@stockport.nhs.uk 0161 419 4784

Quality

(Clinical and Quality Impact Assessment, Please record 'No Impact' if this is the case)

Date of Initial Review	19/11/2021
Date of Last Review	19/11/2021

Area of Impact		Consequence	Likelihood	Total	Potential Impact	Impact (Positive or Negative)	Action	Owner
Quality	Duty of Quality			0	How does it impact adversely the rights and pledges of the NHS Constitution?	No Impact		
					How does the impact affect the organisation's commitment to being an employer of choice?	No Impact		
					What is the equality impact on race, gender, age, disability, sexual orientation, religion and belief, gender reassignment, pregnancy and maternity for individuals' access to services and experience of the service?	No Impact		
	Patient Safety			0	How will this impact on the organisation's duty to protect children, young people, and adults?	No Impact		
					How will it impact on patient safety? • Infection rates • Medication errors • Significant untoward incidents and serious adverse events • Mortality & Morbidity • Failure to recognise a deteriorating patient • Safe staffing levels	No Impact		
					How will it impact on preventable harm? (eg. slips, trips, falls)?	No Impact		
					How will it impact upon the reliability of safety systems? (eg. WHO checklist)	No Impact		
					How will it impact on systems and processes for ensuring that the risk of healthcare acquired infections is reduced?	No Impact		
					How will this impact on workforce capability, care and/or skills?	No Impact		
Experience	Patient Experience			0	What impact is it likely to have on self-reported experience of patients and service users? (Response to national / local surveys / complaints / PALS/incidents)	No Impact		
					How will it impact on choice?	No Impact		
					Will there be an impact on waiting times?	No Impact		
					How will it impact upon the compassionate and personalised care agenda?	No Impact		
	Staff Experience			0	How will it impact on recruitment of staff?	No Impact		
					What will the impact be on staff turnover and absentee rates?	No Impact		
					How will it impact on staff satisfaction	No Impact		

					surveys?			
Effectiveness	**Clinical Effectiveness and Outcomes**			**0**	How does it impact on implementation of evidence-based practice?	No Impact		
					How will it impact on patient's length of stay?	No Impact		
					Will it reduce/impact on variations in care? (eg. readmission rates)	No Impact		
					What will the impact be upon clinical and cost-effective care delivery?	No Impact		
					How does it impact upon care pathway(s)? eg. Mortality	No Impact		
					How will it impact on target performance?	No Impact		
Other	**Please use this section to detail any other impacts to clinical and quality that are not listed in the questions.**							

Data Protection Impact Assessment

The Trust will have to ensure that any third parties used to process or share personal data with will need to ensure the data is secure and confidential and, a data processing agreement or information sharing agreement may need to be in place.

To assess the implications of using personal data, a risk assessment called a Data Protection Impact Assessment (DPIA) is required to ensure the Trust is complying with its legal obligations under the Data Protection Act 2018 and UK GDPR.

If you are doing any of the following you will need to complete a DPIA:

- Setting up a new process using personal confidential data (PCD)
- Changing an existing process which changes the way personal confidential data is used
- Procuring a new information system which holds personal confidential data

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

The DPIA Process:
1) Complete the screening questions below – this is to determine whether or not completion of a full DPIA is required.
2) If a full DPIA is required, you will be advised by the Information Governance Team and sent the full DPIA proforma for completion.

If DPIA's are not completed, there may be data protection concerns that have not been identified which could result in breaching the Data Protection Act / UK GDPR.

Advice/Guidance on completing the screening questions or the full DPIA can be provided by the Information Governance Team by contacting information.governance@stockport.nhs.uk

DPIA Screening Questions

		Yes	**No**	**Unsure**	**Comments** *Document initial comments on the issue and the privacy impacts or clarification on why it is not an issue*
A)	Will the process described involve the collection of new information about individuals?		x		
B)	Does the information you are intending to process identify individuals (e.g. demographic information such as name, address, DOB, telephone, NHS number)?		x		
C)	Does the information you are intending toprocess involve sensitive information e.g.health records, criminal records or other information people would consider particularly private or raise privacy		x		

	concerns?				
D)	Are you using information about individuals for a purpose it is not currentlyused for, or in a way it is not currently used?		x		
E)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		x		
F)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		x		
G)	Does the initiative involve you using new technology which might be perceived asbeing intrusive? e.g. biometrics or facial recognition		x		
H)	Will the initiative result in youmaking decisions or taking action against individuals in ways which can have a significant impact on them?		x		
I)	Will the initiative compel individuals to provide information about themselves?		x		

1. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

If you answered YES or UNSURE to any of the above, you need to continue with the Privacy Impact Assessment. Giving false information to any of the above that subsequently results in a yes response that you knowingly entered as a NO may result in an investigation being warranted which may invoke disciplinary procedures.

DOCUMENT INFORMATION

Type of Document	Policy
Title	Information Sharing & Transfer of Records Policy
Version Number	V 10
Consultation	Digital and Informatics Group
Recommended by	Information Governance & Security Group
Approved by	Information Governance & Security Group
Approval Date	30th November 2022
Next Review Date	November 2023
Document Author	Head of Information Governance & Security/DPO
Document Director	Director of Informatics
For use by	All Trust employees
Specialty / Ward / Department (*if local procedure document*)	

Version	Date of Change	Date of Release	Changed by	Reason for Change
10.0	*Nov 2022*	*Nov 2022*	JC	*Business Group to Division, titles and removal of F&P to DIG*
9.0	*Nov 2021*	*Nov 2021*	JC	*Minor updates to various sections. Updated various sections. Director title, UK-GDPR, Email, new template.*
8.0	*Jan 2021*	*Jan 2021*	JC	*Change of Title for SIRO, Executive statement and Caldicott Guardian.* *Secure Email Guidance updated*
7.0	*Feb 2020*			*Adopted the new Trust Policy Format. Significant layout changes made.*
6.3	*July 2019*			*Further update on secure email domains and external access form*
6.2	*Nov 2018*			*Include references to DPIA and External Access Request Forms* *Replace/reference the new Data Protection Act 2018 and GDPR.* *Remove Information Sharing Protocol from Appendix.* *Additional information about secure government and NHS email standard*
6.1	*Aug 2018*			*Clarification on sending information via the internal mail (specifically to take account of staff working in the community)*
6.0	*May 2018*			*GDPR inclusion*
5.0	*April 2017*			*Refresh of Policy*

				Clarification of Secondary Use purpose *Clarification of procedure when using royal mail*
4.3	*Oct 2015*			*Clarification over secondary use requirements* *Update to secure e-mail domain information* *Clarification around sharing PID internally*
4.2	*July 2015*			*Updated to include information on posting health records; information security when transporting information off site*
4.1	*March 2015*			*Updated information relating to NHS encryption facility* *Inclusion of Secure File Transfer information*
3.1	*May 2014*			*Included definitions for primary and secondary uses, pseudonymisation, responsibility of Information services department and a section on pseudonymisation process*
3.0	*February 2013*			*Renamed to clarify scope, previously Information Sharing & Safe Haven Policy. ISP reviewed.*
2.2	*September 2011*			*Minor alterations to leaflet and ISP.*
2.1	*September 2011*			*Inclusion of further detail in relation to NHS mail and clarification of where encryption should be applied manually.*
2.1	*September 2011*			*Section 2 - Inclusion of first paragraph for clarification around the scope of the document. Other minor amendments to wording.*
2.0 (Final)	*March 2011*			*Inclusion of an Information Sharing Protocol template at appendix (b)*
2.0 (Draft)	*January 2011*			*Adopted the new Trust Policy format.* *Significant Changes Made.* *Including inclusion of definitions; requirements around telephones, transportation and whiteboards; change to the official Safe Haven location; further details of the legal requirements of information sharing and; implementation and monitoring arrangements.*
1.2	*October 2008*			*Significant Changes Made.*
1.0	*March 2006*			*New Policy*