Transfer of Information and Safe Haven Policy

Author:	Interim Information Governance Manager and Acting Data Protection Officer (DPO) Rachel Adams
Document Owner:	Executive Director of Operational HR & OD Leon Hinton
Revision No:	5
Document ID Number	POLCGR077
Approved By:	Information Governance Group
Implementation Date:	December 2018
Date of Next Review:	November 2021

Best of care
Best of people

Transfer of Information and Safe Haven Policy

Document Control / History	
Revision No	**Reason for change**
New	New Policy Update on confidential personal identifiable information – see section 11.6.
1	Annual review and addition of equality impact assessment
2	Review and addition of monitoring table
3	2 yearly review, change of job titles
4	2 yearly review
5	Change of title, and 2 yearly review

Consultation
Information Governance Group members

Table of Contents

To be read in conjunction with any policies listed in Trust Associated Documents.

1 Introduction

1.1 This policy lays out the practical methods that need to be applied in undertaking a transfer of data, and will provide additional guidance more specifically on the transfers of controlled data. This policy is applicable to anyone handling Trust information that may have a need to transfer Trust data, including:

- employees of the Trust
- contractors
- agency staff
- contractual third party suppliers
- agents and partners of the Trust

1.2 There are many occasions when transfer of Trust data is required between internal departments, third party service providers, public bodies, commercial organisations and individual officers to perform business functions.

1.3 It is essential that any transfer is done in a way that is appropriate for the type of data being transferred.

1.4 If the information is personal or special category data as defined by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 or considered business confidential it is essential that the transfer is performed in a way that adequately protects the information.

1.5 Article 25 (Data protection by design and by default)of the GDPR now includes the requirement of organisations to ensure that the Trust considers the right of Data subjects when transferring information and ensuring that that data mineralisation is used when appropriate for example the use of pseudonymised, or anonymised data.

1.6 Data can potentially be transferred in a wide variety of media and methods both into and out of the council, in electronic and/or paper format. In every transfer there is a risk that the information may be lost, misappropriated or accidentally released. Where this data is controlled data, this represents a risk to the Trust of breaching our responsibilities under the GDPR and could lead to regulatory action by the Information Commissioners Office (ICO), including significant fines.

2 Purpose / Aim and Objective

2.1 This policy sets out the main methods / media that can be used for transferring or sending personal information and the minimum requirements that must be followed.

2.2 If any staff members are unsure about what method to use for sending or transferring information they can contact their line manager, Head of Department or the Information Governance Team for further advice.

2.3 At no point should a team use a new way of transferring information without it first being signed off by the Information Governances team or IT.

2.4 For all transfers of all personal information it is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender. In line with the GDPR and the Caldicott Principles (see appendix for more information)

Computers

2.5 PCs should be located so they are not in direct line of patients or family members.

2.6 At no point should you allow patients or family members to use work computers or laptop for personal reasons.

2.7 Laptop should be secured at all times and locked away in offices or drawers when not in use.

2.8 Should you find your PC or laptop is not working this must be reported to the IT service desk.

2.9 Do not share password access to computers or systems which contain Personal Confidential Data.

2.10 Be vigilant when you visit a website that is declared “untrusted”. If a web browser states that you are about to enter an untrusted site, be very careful; it could be a fake phishing website that has been made to look like genuine. A browser may display a red padlock or a warding message stating your connection is not private

2.11 You should lock your device as soon as you stop using it. ALL mobile phones, laptops, PCs and tablets, whether personal or not, should have a passcode set. If you see a colleague's device open and unlocked, lock it for them and gently remind them to do so in future.

2.12 This also applies to corporate mobile devices - activate the lock function so that a password or code is needed to unlock them.

2.13 Further guidance can be found in the Information Security Policy.

Electronic Mail

2.14 Email can be the most efficient option for exchanging information securely but as with all forms of information transfer, there are risks.

2.15 The increased risk of cyber attached is the reason that Medway foundation use used NHSmail which is automatically encrypted in transit; therefore mail between NHS.net accounts is secure.

2.16 At no point are staff employed or working for Medway Foundation Trust allowed to use personal emails to transmit patient, staff or confidential information using personal emails.

2.17 It is recommended to use “generic (or shared) mailboxes” for the transfer of personal confidential data which supports a regular business process.

2.18 The following checks/precautions should be carried out by the sender at all times when transferring personal information by e-mail:

- Check whether it is acceptable to send personal information.
- check that everyone on the copy list has a genuine ‘need to know’.
- use the minimum identifiable information (e.g. NHS number).
- Check encryption requirements.
- Always double check that the name and e-mail address of the recipient are correct.
- The Email message must contain clear instructions on the recipient’s responsibilities and instructions on what to do if they are not the correct recipient.
- Check with the recipient that his / her e-mail system will not filter out or quarantine the transferred file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.
- Ensure that the information within the e-mail is stored in the agreed format for the record type i.e. in line with professional record keeping guidelines.
- Never give your login details to anyone.
- Ensure that a signature block is used on all emails so should it be received by the wrong person they know who to contact

2.19 Hackers and criminals sometimes use unsolicited emails containing attachments or links to try and trick people into providing access to information.

2.20 Attachments may contain a file with an .exe extension, these files are executable, and some may contain malicious software (malware) that will automatically download onto your computer.

Phishing

2.21 This type of threat is known as phishing. Phishing is by far the biggest and easiest form of social engineering.

2.22 Criminals use phishing emails and websites to scam people every week. They are hoping for you to click on fake links to sites or open attachments so they can steal data or install malicious software.

2.23 The aim of phishing emails is to force users to make a mistake – for example, by imitating a legitimate company's emails or by creating a time limited or pressurised situation.

2.24 Phishing email attachments or websites might ask you to enter personal information or a password – or they could start downloading and installing malware.

2.25 If you receive a request from a supposed colleague asking for login details, or sensitive, financial or patient/service user information, you should always double check the request with that colleague over the phone.

2.26 Equally if you receive an unsolicited email that contains attachments or links you have not asked for, do not open them. Remain vigilant and report the suspicious email to the IT service desk

Electronic memory and removable devices, (CD, DVD, Floppy, USB drive, Memory Card)

2.27 It is now becoming more common for information to be sent in electronic format. Staff must ensure that the following instructions are followed

2.28 Only trust provider removal media is used to ensure that it follows the trusts encryption requirements

2.29 Personal Information must be enclosed in a file and encrypted using a product approved by the Trust.

2.30 If the information needs to be posted, it must be sent using an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

2.31 Any attachment is required to be password protected.

2.32 Any password must be to organisation standard. 7 characters, mix of alpha and numeric.

2.33 Any password to open the attached file must be transferred to the recipient using a different method than email, e.g. a telephone call to an agreed telephone number, closed letter.

2.34 An accompanying message must contain clear instructions on the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.

2.35 Any accompanying messages and the filename must not reveal the contents of the encrypted file.

2.36 The sender must check at an appropriate time that the transfer has been successful, and report any issues to his/her line manager.

Fax Transmission

2.37 By March 2020 all fax machines will be banned from the NHS.

2.38 Fax is inherently insecure and is not recommended for the transfer of personal information. It is always safer to share information using the internal e-mail system and should only be used if there is no other way of getting urgent information to another organisation. If this is the case the following guidance must be followed in all cases:

- The sender must check that the Fax number is correct and that the receiver is awaiting transmission.
- Use a fax cover sheet.
- For personal information the number must be double-checked by a colleague before transmission and telephone contact must be maintained throughout transmission.
- Minimal information should be sent
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine and a clear requirement to securely destroy the message when no longer required.
- The message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

Manual transfer of records

2.39 Patient records should only be sent off site by the patient service centre for appointments at other hospital.

2.40 Patients being transferred to hospices, other hospitals and nursing homes should be sent with copies of the most recent encounter and relevant clinic letters. Full notes should not be sent off site without direct promise from senior management

2.41 Notes being transported around the hospital must be taken in appropriate carts.

2.42 Carts should never be left unattended outside of offices and the top records should be facing downwards to prevent patient information from being seem.

2.43 Care should also be taken with Corporate records and should only be removed from Trust premise when the Transfer has been authorised.

In person

2.44 Staff should also take care when carrying one off pieces of paper, should you reach your next appointment and find information has been lost you must track back your steps. If you are still unable to find the information it must be reported via Datix

2.45 No information should be removed from the site unless its for direct patient care or authorisation has been given by line management. Should you have to take information home with you overnight information must be kept locked away and not left in cars or in locations that could leave to others in your household from accessing the information.

Physical location and security

2.46 Do not allow unauthorised persons into areas where confidential information is processed. Be aware of people tailgating when going through doors.

2.47 Security and fire doors should be kept locked at all times and not left wedged open even in the summer. This does not only cause information governance issues but also security and fire hazards.

Passwords

2.48 At no point should passwords be written down in notebooks, diaries, post-it notes or on the back of ID badges.

2.49 Passwords should never be shared with colleagues, this includes smart cards.

2.50 Passwords should be a mixture of upper and lower case letter, numbers and symbols.

Post

2.51 Incoming mail should be opened away from public areas.

2.52 Outgoing mail (both internal and external) should be securely sealed and marked 'private and confidential' if it contains Personal Confidential Data. Further this should be sent by a secure mail method such as signed for or registered mail.

2.53 Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel.

2.54 Mark the envelope/parcel, private and confidential and add a return address and contact details, unless this will directly compromise confidentiality.

2.55 Packages must be received and signed for by the addressee.

2.56 The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

2.57 When placing letters in envelopments staff should take care to ensure that any supporting documentation such as results or test forms are for that patient.

Telephone

2.58 Telephone conversations are one of the most common ways for people to try and inappropriately acquire information. When you are talking to a professional do not be afraid to tell them that you will call them back on their main switch board number or ask them to send you an email.

2.59 Ensure that

- the caller or called person is identified before discussing sensitive data and disclosing the reason for the call
- the enquirer has a legitimate right to have access to the information before disclosure is made
- Do not make telephone calls which require identifying details and/or sensitive data in an area which you can be overheard (for example in Reception).

2.60 Services that have voicemail capability need to ensure that the message is kept up to date and messages are retrieved in a timely manner.

Text messaging (SMS), instant Messaging (IM) and forward app

2.61 Due to increased use of mobile phones, text messaging (SMS) and Instant Messaging such as WhatsApp and Facebook Messenger is now being considered as a way of staff communicating with patient/service users.

2.62 No personal information should be sent using the above methods without express agreement from the Information Governance Team who will require a privacy impact assessment to be undertaken prior to any sharing of personal information takes place.

Disposal of confidential information

2.63 All IT assets should be disposed of via the IT service desk example can be found in 3.4.

2.64 All paper information should be disposed of via the red confidential waste bins. Information should not be left under ward clarks desks or via the normal black bins.

Information Sharing Agreements

2.65 All regular sharing of personal information should be subject to an Information Sharing Agreement (unless the Information Governance Team confirms that an agreement is not required). Further advice and guidance on this can be sought from the Information Governance Team.

Data Flow Mapping

2.66 This describes departments where there are routine information flows of personal confidential data. The requirement to map information flows is included in the Data Security and Protection Toolkit (DSP). Information flows are reviewed annually and further guidance is provided on the information governance intranet page

3 Definitions

3.1 Data Protection Act 2018/General Protection Regulations 2016 or any subsequent legislation to the same effect - The law around how personal information should be managed by all organisations that use, store and process personal information.

3.2 Caldicott Principles - A set of principles that lay out how patient information should be handled by NHS organisations to ensure confidentiality is upheld.

3.3 Freedom Of Information Act 2000 - A law that gives certain rights to individuals to request access to information held, stored and processed by certain public organisations including Health Boards.

3.4 Removable Media-Is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs/DVDs, USB flash memory sticks or pens, PDAs,tablets, and smart phones/devices

3.5 Safe Haven Is a location which is set up to receive and manage confidential information appropriately. It may be a post room or a fax machine in a secured room with restricted access, or anywhere were personal information may be taken and held securely before being passed onto the appropriate recipient.

4 (Duties) Roles & Responsibilities

4.1 Trust Board

- The Trust Board is ultimately responsible for ensuring that the Trust corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.
- The Trust Board is responsible for approving the Trust's Corporate Policy for information governance.
- The Trust Board is responsible for reviewing reports from the SIRO, Data Protection Officer[1] (DPO) and Caldicott Guardian to the Board on information governance arrangements.
- The Trust Board is responsible for understanding the statutory framework and assuring itself on the adequacy of the Trust arrangements for meeting requirements.

4.2 Chief Executive

- The Chief Executive has overall responsibility for ensuring that sufficient resources are provided to support information governance requirements.

[1] As assigned under the General Data Protection Regulation

4.3 Caldicott Guardian

- The Medical Director is the Trust's Caldicott Guardian who is responsible for ensuring that MFT satisfies the highest practical standards for handling patient identifiable information. The role encompasses:
    - acting as the 'conscience' of MFT;
    - facilitating and enabling information sharing and advising on options for lawful and ethical processing of information;
    - representing and championing Information Governance requirements and issues at Board level;
    - receiving training as necessary to ensure they remain effective in their role as the Caldicott Guardian;
    - ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and
    - overseeing all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

4.4 Director with IG portfolio responsibility

- Is the designated Director for Information Governance with responsibility for ensuring that the Trust has plans and policies in place to fulfil the requirements of the statutory framework;
- Is the Chair of the Information Governance Group, ensuring upward reporting to the Executive Group;
- acts as champion for information risk on the Board and provides written advice to the Accounting Officer on the content of the Organisation's Annual Governance Statement in regard to information risk;
- understands how the strategic business goals of MFT and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed;
- implements and leads the NHS Information Governance risk assessment and management processes within MFT;
- advises the Board on the effectiveness of information risk management across MFT; and

4.5 Information Governance Group

- This Group is established on the authority of the Executive Group to assist the Trust Board in fulfilling its responsibilities in relation to information governance. Its purpose is to monitor and co-ordinate implementation of the Information Governance Policy and the DSPT - requirements and other information related legal obligations. Terms of Reference setting out the full responsibilities of the Group are available here.

4.6 **Director of IT Transformation and Senior Information Risk Owner (SIRO)**

- Responsible for the management and accountability of information risk for the organisation.
- The formulation and implementation of IT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust IT security arrangements in line with best industry practice;
- Effective management and security of Trust
    - resources, for example, infrastructure and equipment;
    - Developing and implementing a robust IT Disaster Recovery Plan;
    - Ensuring that IT security levels required by NHS Statement of Compliance are met;
        - Ensuring the maintenance of all firewalls and secure access servers are in place at all times, and;
        - Ensuring the provision of Information Asset Owners for the IT infrastructure with specific accountability for computer and telephone equipment and services that are operated by corporate and clinical work force, e.g. personal computers, laptops, personal digital assistants and related computing devices, held as a NHS asset.

4.7 **Chief Operating Officer (Planned Care)**

- The Chief Operating Officer (Planned Care) is responsible for the management and delivery of the function of health records management in accordance with information governance policies.

4.8 **Information Asset Owners (IAO), who will:**

- lead and foster a culture that values, protects and uses information for the success of MFT;

- know what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset;
- receive training as necessary to ensure they remain effective in their role as an Information Asset Owner;
- know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy; and
- understand and address risks to the asset, and provide assurance to the SIRO.

4.9 **The Data Protection Officer (DPO):**

- Must ensure the Trust is GDPR is compliant at all times and takes into consideration any new legislation that might take effect from time to time.
- Has responsibilities to ensure requests under the GDPR, including Subject Access and the other Individual Rights are completed in a timely manner.
- Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.
- Is responsible for liaising with external organisations on GDPR
- Is responsible for ensuring the board is kept up to date

4.10 **The Information Governance Manager, who will:**

- maintain an awareness of Information Governance issues within MFT
- act as the operational lead for delivery of the Information Governance agenda;
- Manage the information governance team;
- review and update the suite of Information Governance policies, strategies, framework and guidance in line with local and national requirements;
    - review and audit all procedures relating to this policy where appropriate on an ad-hoc basis; and
    - ensure that staff are aware of the requirements of the policy.

4.11 **Information Governance Team & Partner Subject-Matter Experts**

- The Information Governance Team are responsible for:
    - Providing expert advice and guidance to all staff on all elements of Information Governance.

- Developing internal Information Governance policies and procedures to meet NHS information governance guidance and legislation.
- Developing Information Governance awareness and training programmes for staff.
- Ensuring compliance with Data Protection, Information Security and other information related legislation.
- Co-ordinating the response to freedom of information requests.

4.12 **Line Managers**

- Line managers are responsible for ensuring that the Information Governance Policy is implemented within their group or directorate.

4.13 **All Staff**

- All staff are responsible for adhering to the policy and fulfilling mandatory training requirements.

5 Monitoring and Review

What will be monitored	How/Method/ Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions
The Policy	Every two years or more frequently if appropriate to take into account changes to legislation that may occur and/or guidance from the Department of Health, the Information Commissioner's Office and/or any relevant case law	Information Governance Manager	DPO	Information Governance Group
Database registration	Annual audit of databases	Information Asset Owners, Head of Clinical Systems Development,	Senior Information Risk Owner	Information Governance Group

What will be monitored	How/Method/ Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions
		& IG Manager		
Mandatory Information Governance Training	Half yearly reports to Exec Group as part of SIRO report	Information Governance Manager Senior Information Risk Owner	Exec Group	Directorates and Line Managers
Incidents and Outcomes	Reports to every meeting of Information Governance Group (meets at least quarterly) Half yearly SIRO reports to Exec Group	Information Governance Manager Senior Information Risk Owner DPO	Senior Information Risk Owner Exec Group	Information Governance Group
Compliance with Data Protection	Meta-compliance questions to randomly selected staff. Spot checks around Trust	Information Governance Manager Information Governance Manager	Information Governance Group	Information Governance Group

6 Training and Implementation

6.1 All staff are required to complete their annual Data Security and Protection training either on-line or through classroom based sessions. Bespoke training is also available upon request.

6.2 Compliance with this policy is monitored via:

- The percentage level of staff completing training
- Monthly management information on the level of subject access requests completed within the statutory deadline
- The level of data breach incidents reported via Datix
- The level of data breach incidents escalated to the ICO via the IG Toolkit

Failure to adhere to the policy will lead to HR investigation and potential fines of up to £17.5 million for the organization.

7 Equality Impact Assessment

All public bodies have a statutory duty under The Equality Act 2010 (Statutory Duties) Regulations 2011 to provide “evidence of analysis it undertook to establish whether its policies and practices would further, or had furthered, the aims set out in section 149(1) of the [Equality Act 2010]”; in effect to undertake equality impact assessments on all procedural documents and practices. Authors should use the Equality Impact Toolkit to assess the impact of the document.
In the first instance this will mean screening the document and, where the screening indicates, completing a full assessment. The Toolkit can be found on the Trust website http://www.medway.nhs.uk/our-foundation-trust/publications/equality-and-diversity/equality-impact-assessments/

A document will not be considered approved until the author has confirmed that the screening process has been carried out and where required a full impact assessment has been completed. Where a full assessment is completed this should be submitted along with the document for approval.

8 References

Document	Ref No
References:	
Access to Health Records Act 1990 Access to Medical Reports Act 1988 Children Act 1989 Computer Misuse Act 1990 Confidentiality NHS Code of Practice November 2003 Copyright, Designs and Patients Act 1988 Crime & Disorder Act 1998 Electronic Communications Act 2003 Freedom of Information Act 2000 General Data Protection Regulation 2018 Health and Social Care Act 2001 Human Rights Act 1998 National Health Service Act 2006 (Section 251) NHS Code of Practice, Records Management NHS Information Governance – Guidance on Legal and Professional Obligations Sept 2007 Police and Criminal Evidence Act 1984 Regulation of Investigatory Powers Act 2000	
Trust Associated Documents:	
Information Security Policy	POLCGR018
Remote Access Policy	POLCGR084
Network Security Policy	POLCGR082
Acceptable Use of Trust Information Assets	POLCGR113
Secure Transfer of Information Policy	POLCGR077
Information Governance Policy	POLCGR017
Information Governance Strategy	STRCGR013

Appendix 1 – The Principles of the GDPR and the Caldicott principles

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1)[2], not be considered ot be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. .
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processes; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
- 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.

The controller shall be responsible for, and be able to demonstrate compliance with, the above principles.

[2] Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Caldicott Principles

Use of Caldicott Principles when transferring personal information, before transferring any personal information the Caldicott Principles should be applied. These are:

- Justify the purpose for which the information is needed.
- Only use personal information when absolutely necessary.
- Use the minimum personal information possible.
- Access to the information should be on a strict need to know basis.
- Everyone should be aware of his / her responsibilities to respect the confidentiality of personal information.
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.