North East Ambulance Service NHS
NHS Foundation Trust

Secure Transfer of Information Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-11
Version Number	3
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	15 February 2017
Date Policy Effective From	08 March 2018
Next Review Date	08 March 2021
Keywords	data, safe haven, information assets, bulk transfer, routine flows, NHS Mail, encryption, information sharing agreements, removable media

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control – Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
1	All	'NEAS' replaced with 'Trust'. All document references removed. Updated committee references.	Information Governance Manager	14 February 2014
1	5.6.1	PTS Control, Resource Scheduling and A&E Control replaced with Contact Centre.	Information Governance Manager	15 September 2014
1	EIA	It was suggested that the acronyms EIA and EIS should be expanded for clarity (to Equality Impact Assessment and Equality Impact Screening) – cannot change as this is part of the template.	Information Governance Manager	22 September 2014
2		Q-pulse numbering changed due to restructuring of the system and review date set at previous revision and table of revision amended to reflect change along with version numbers		19 January 2016
3		Policy name changed to ''Secure Transfer of Information Policy''. Contents updated to reflect GDPR and new DP Bill	Information Governance Officer	Feb 2018

This page should not be longer than one single page.

Table of Contents

1. Introduction

The North East Ambulance Service (Trust), like other NHS organisations, has a legal duty to keep all personal and confidential information secure. This duty originates from common law, data protection and human rights legislation.

All staff within the Trust must therefore safeguard the integrity, confidentiality, and availability of information.

This policy provides staff with guidance on how to transfer information securely in line with national and local best practice and legislative requirements, e.g. secure email transfers and encryption (see Data Encryption Policy).

Transferring information may be on an individual basis or as a bulk transfer. Examples of information transfers include:

- Transfer of patient report forms from an ambulance station to headquarters.
- Several person-identifiable electronic records sent via email to somebody outside the organisation.

The Trust is also obliged to identify, map and risk assess routine transfers of person identifiable and sensitive information in all areas ensuring risks are appropriately recorded in the risk register along with the actions taken to secure the information.

2. Purpose

The overall purpose of this policy is to inform staff on best practice when securely transferring information. This is to reduce the risk of unauthorised disclosure of such information that could lead to a breach of confidentiality. The policy requires staff to consider the various methods available to transfer information and to ensure that security provisions are applied to every selection.

The policy also identifies the risks when transferring personal information and requires staff to consider these in line with legislation.

3. Scope

This policy covers all aspects of information existing within the Trust including, but not limited to:

- Patient / client / service user information
- Staff Information
- Corporate Information

The policy applies to any individual employed, in any capacity, by the Trust, volunteer or contractor who holds a Trust domain account.

This policy covers all methods of transferring information, including, but not limited to:

- Email
- Post
- Telephone / answer phone
- Computer systems / electronic media

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the proper use and security of Trust systems. Implementation of, and compliance with the policy is delegated to the Director of Finance and Resources.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

The SIRO is also responsible for making sure the trust meets all legislative requirements in relation to information security.

4.4 Information Governance Manager

Has responsibility for:

- Developing, maintaining and implementing this policy;
- Maintaining a register of all information assets containing personal information.
- Maintaining a register of all information flows.
- Monitor breaches in information flows and report to managers where breaches in security are identified.
- Implement secure processes to protect personal information transfers.

4.5 Line Managers

Have a responsibility to ensure all current, new and temporary staff attend induction programme and receive mandatory Information Governance Training on an annual basis.

4.6 All staff

All staff have a responsibility to:

- All users are personally responsible for ensuring that they are aware of and compliant with this policy. By signing up to a Domain Account, users will agree to this policy and its guidelines and should be aware that a breach of this policy may be regarded as serious misconduct which would lead to disciplinary action or dismissal in accordance with disciplinary procedures.
- Bring to the managers attention areas of concern regarding the secure transfer of information.

Seek advice from the Information Governance Manager when unsure about the most appropriate and secure methods of transferring information.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Bulk Transfer	Defined as the transfer of 51 or more electronic or paper records.
Cloud Services	Cloud services are defined as services provided by an external supplier and made available to organisations, or individuals, on terms and conditions, which are defined by the external supplier. Cloud services are provided by infrastructure outwith the organisation's domain (data centres). Cloud storage services facilitate the sharing of files and make data available over a range of computers and other mobile devices, usually accessed via options including: web browser; mobile app; synchronisation client; drive mapping. Cloud storage provider examples include: Dropbox, Box, Microsoft OneDrive, Apple iCloud, Google docs.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Information Assets	Information Assets include: • Information e.g. content within databases, archive and back-up data, audit data, paper record. • Software e.g. application and system software, development and maintenance tools. • Hardware e.g. PCs, laptops, USB sticks, PDAs. System / process documentation e.g. system information and documentation, manual and training materials, business continuity plans.
Information Sharing	A set of common rules binding on all the organisations involved in a data sharing initiative. It is not contractually

Term	Description
Agreements	binding but is used to set good practice standards that the parties need to meet in order to fulfil any duty of care which exists in relation to the regular/routine sharing of personal information.
Personal data	Information relating to an identified or identifiable natural person ('data subject'). an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.[1]
Removable Media	A term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. USB sticks, CDs / DVDs, PDAs.
Routine Flows	Any flows or transfers of information that are undertaken on a regular basis; 'regular' in this context could be as infrequently as once a year.

6. Policy Content

6.1 Legal and professional obligations

The Data Protection legislation requires that "Appropriate technical and organisational measures shall be taken to make data secure". The EU General Data Protection Regulation (GDPR) 2016 (Article 32 – Security of processing) emphasises that the controller and processor shall implement appropriate technical and organisation measures to ensure a level of security appropriate to the risk. NHS Code of Practice: Confidentiality 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".

6.2 Risks in transferring information

There are a number of risks associated with transferring information. Examples of such risks include:

- Information being lost, damaged or intercepted in transit e.g. stolen laptops, lost memory sticks, opened envelopes.
- Information sent to the wrong address via e-mail or post.
- Confidential conversations being overheard.
- Information not being disposed of appropriately.

In order to minimise the risks, staff must carefully choose the most appropriate method of transferring information. In general the following criteria must be

[1] EU General Data Protection Regulation 2016

considered for the transfer of information in both hardcopy and digital formats:

- Adequate protection from interception, copying, modification, misrouting and destruction. Please refer to Clinical Records Policy when tracking records between stations and HQ. In the case of digital information (including email file attachments) this includes protection from malicious code.
- Assurance measures such as physical spot checks of compliance with policies and procedures, technical monitoring of communication traffic.
- Assurance measures, such as incident reporting analysis to evaluate the effectiveness of the security controls in place.

Whilst the transfer of all information has risks, bulk transfers (see glossary) are generally considered the greatest risk. Should these risks occur and security/confidentiality of information is compromised, there is an impact on the following:

- Individuals – whose information has been put at risk.
- Staff – whose actions placed the information at risk and may have breached local policy, which could lead to disciplinary action. There may also be legal implications if they have breached data protection legislation.
- Organisations – a breach of confidentiality may have an impact on the organisation in terms of reputational damage or lack of trust or confidence from the public and could lead to potential prosecution under information legislation. The Trust may also incur a monetary penalty from the Information Commissioners Officer under legislation. All information security incidents relating to the transfer of information must be reported following the Trust risk and incident reporting procedure. All IG related risks are regularly reviewed by the Information Governance Working Group via the Information Governance Risk Register.

It is important that all staff report any incidents in regards to the transfer of information to avoid similar incidents reoccurring but also so constructive action can be taken and lessons learnt shared.

6.3 Considerations and methods of transfers

Before securely transferring information, there are a number of considerations to be made in order to decide which method of transfer is the most appropriate and secure. Careful consideration must be given based on the:

- Type / format of information
- Location of the information to be transferred to and from
- Amount of information to be transferred
- Types of methods of transfer available
- Speed of delivery
- Cost
- Potential risk to the method of transfer
- Patient / service user choice

Depending on the above considerations, the following methods are available to transfer information.

- E-fax
- Email
- Secure electronic transfer
- Post
- Internal mail
- Verbal communication, e.g. telephone
- SMS Text message
- Other methods of transfer

6.3.1 Fax machines

The Trust's safe haven fax machines are sited in areas that are restricted to those who need to access the information i.e. away from public areas and in a locked room or in an area / building accessible by a key pass.

The Trust safe haven fax machines can be found in the following area:

- Contact Centre

Please note that a log will be kept for Safe Haven fax use.

Person-identifiable information must only be sent by fax when absolutely necessary. If the recipient is another NHS organisation, the information must be sent to its safe haven fax (the numbers of which are contained in the Safe Haven Directory at:

http://systems.hscic.gov.uk/data/ods/searchtools/safehaven/index_html

The following points must be adhered to:

- Preset (autodial) should be programmed into the fax machine in preference to manual dialling to minimise risk of misdialling.
- Use a fax cover sheet that contains a confidentiality statement, for example:

"This fax is confidential and intended only for the individual or entity to whom it is addressed. If you are not the intended recipient (or responsible for delivery) of this fax and its attachments, please notify the sender and destroy the transmission and any copies made. The confidentiality of this fax cannot be guaranteed unless the contents are exempt from the FOI Act 2000."

Where a safe haven fax does not exist, it is best practice to:

- Verify the fax number with the recipient.
- Contact the intended recipient to ensure they are available and to allow them to prepare to receive the fax within the agreed timescale e.g. for non-routine flows.

The responsibility for the correct despatch of all fax messages rests with the sender. If there is any doubt do NOT send the document by fax transmission.

Ensure a code or password is used if the facility exists on the machine.

Staff working in the safe haven area, must forward confidential information to the recipient in a sealed envelope, marked ‘Confidential’.

6.3.2 Email

The strategic NHS email system ‘NHSmail’ (xxx.xxx@nhs.net addresses) has been designed to ensure the security and confidentiality of NHS information in transit between account holders and benefits through the integration of strong encryption technology that automatically encrypts messages in transit.

NHSmail is currently the only NHS approved method for exchanging patient data by email, but only if both sender and recipient use an NHSmail account or if sending to another government secure domain (see Email Policy)

If the recipient is outside of the NHS.net email system, the encryption facility can be used to encrypt the message - advice can be sought from the IM&T Service Desk.

The Trust’s Email policy gives more guidance on access and use of Email system.

6.3.3 Removable media

Information may be transferred via an encrypted, Trust approved USB device, any other removable media such as an encrypted CD, DVD, PDA or pens depending on the nature of the requirement for transfer and volume of data to be transferred.

Users will only be allowed to write to approved, Trust-owned hardware-encrypted devices. A staff requiring access to any removable media should contact IT Service Desk.

More information available on Data Encryption Policy.

6.3.4 Secure File Transfer Protocol (SFTP)

A Secure File Transfer Protocol is a program used to transfer files up to other organisations. All requests for setting up a SFTP to receive or transfer information/data should be via the IT Service Desk in conjunction with Information Governance. It is advisable to seek guidance from IT Service Desk and Information Governance if you are required to transfer data to a SFTP set up by another organisation.

6.3.5 Post

The chosen transfer method should be adequately secure and cost effective. It may be acceptable to the organisation to routinely post letters which contain the details of one service user but this may not be acceptable for a letter containing sensitive details of a number of identifiable service users. The Trust expects that the first choice of transfer of regular communication would be via secure email (example, contract of Employment, OH information) unless it is a legal requirement to use another method.

All outgoing post should be taken to the post room in the reception area and clearly marked according to the information’s classification i.e. private and confidential, for addressee only.

Pigeon holes are adjacent to the postal room and supervised by postal and reception

staff. It is the responsibility of all staff to ensure pigeon holes are frequently checked and post is collected.

Incoming post should be opened away from the public areas and in a secure area.

Patient health records and other records, including correspondence etc., must be handled and stored in a secure fashion. Detailed procedures relating to the collection, transportation, sharing, retention and disposal of patient clinical records are contained within the Records Management Policy.

No sensitive records may be stored in unsupervised public areas at any time.

Items not marked with a name or department, and are not labelled 'Private & Confidential' should be opened by the post staff to establish whom it belongs to.

Any unmarked items that contain person-identifiable information should be placed in a sealed envelope and passed to the appropriate individual. Staff should treat this as an information security breach and complete an incident report form in line with the Trust policy.

If there is any question as to the appropriateness in respect of the above, then the item(s) should be placed in a sealed envelope and passed to the Information Governance Manager. This applies equally to mail sent internally as it does externally.

6.3.6 Internal mail

When records are sent in the internal post an assessment must be made as to the risk of loss. If the loss of those records could compromise patient care or create a serious breach of confidence the following procedure must be followed.

Records must be transferred in an envelope which can be securely sealed, be clearly addressed to a named individual including their title and location and be marked Private and Confidential. If an envelope is reused cross out the previous address.

If staff need to send records urgently then they should contact the intended recipient in advance to ensure that they are not on leave or working away from their base.

All staff should consider email as their first option for transferring information. For example, any personal documents such as driving license, training documents etc. should be scanned and emailed to the appropriate department (from work email) instead of relying on internal post which has more chances to go missing.

6.3.7 Verbal communications, including telephones

Requests for person-identifiable information from other parts of the NHS must be verified to confirm the person making the request has a right to know before release of any sensitive information.

Person-identifiable information should not be discussed on telephones that have 'hands free' capability unless they are situated in a single user office or car, and only those persons who need the information are present. Headsets should be used in the Control Room so that only the Control Assistant is aware of the information being

passed.

Requests for information under both the Data Protection legislation and the Freedom of Information Act 2000 cannot be transferred over the telephone. The caller must be asked to make their request in writing and the responses will follow the medium the request has come in (eg. Email/post) unless otherwise specified.

Requests for information from the press or media must be forwarded on to the PR and Communications Officers.

Requests from Police should be accompanied by a Police Request for Personal Information Form and appropriate guidance should be followed for example, logging the request in Ulysses.

The following steps should be taken when person-identifiable information is requested over the telephone:

- Confirm the name of the person making the request along with their job title, department and organisation (if applicable).
- Establish the reason for the request.
- Take a contact telephone number. This should be a main switchboard number not a mobile or direct line number.
- If you are in any doubt of the caller's identify, call them back.
- If in doubt, check the information can be released and telephone the caller back.
- Provide the information only to the person making the request – do not leave a message either with somebody else or on an answering machine.

6.3.8 SMS text messages

There are various potential applications for text messages in the provision of services, e.g. service user appointments. The benefits of using text messages to convey information must be weighed against the risks. Key considerations when using text messages are:

- Is the mobile phone number correct?
- Is the mobile phone receiving the text message being used by the intended recipient of the message?
- Has the message been received, and what provision is there to audit message receipt?

Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) - as mobile phones are easy to misplace or may get stolen, there is a danger of a breach of confidentiality occurring that the patient / service user may find distressing or damaging.

Text messages should not be used to convey sensitive information and the use of text messages for the transfer of data should be kept to a minimum, e.g. an appointment reminder does not need to include the name of the specific clinic.

When consent is sought for appointment reminder services, service users should be informed of what information will be included in standard SMS messages sent to them

via the service and the option to opt out must be available on request.

6.3.9 Cloud storage

Where there is a requirement to share information with others using a cloud storage service, then it is important that individuals who enable the sharing of data do so with the following safeguards:

- Grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the *correct* individuals.
- Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honour all security requirements as well as privacy and confidentiality commitments.

All access to Cloud based storage should be approved by the Information Governance Manager upon submitting a Service Desk Request with valid justification. These requests will be assessed individually on risk vs requirement basis. Any high risks will be recorded in the Risk Register of the particular department.

6.4 Other methods of transfer

This policy highlights the main ways in which the transfer of information is likely to be transferred. The same careful considerations must be applied to all methods of transfer, particularly in regards to the security and confidentiality risks when transferring information. Further advice or guidance is available from the IG Team.

6.5 Paper records taken away from Trust premises

All staff must seriously consider the need for taking person identifiable records out of their base with them. This should only happen when absolutely essential and there is no other method available for accessing/recording the information required. Staff must not carry around more information than is necessary.

It is recognised that it may be necessary to remove records from their base and the guidelines below should be followed to reduce the risk of the records being accessed by an unauthorised person, lost or stolen. These guidelines are also applicable to HR staff transporting staff records.

- Only take the minimum amount of information required and consider whether you actually need the notes in order to carry out your work.
- Records should not be removed for general administration purposes, e.g. writing routine reports.
- Information sent via email should under no circumstance be printed and removed from Trust premises.
- Record the removal and return of files taken away from the workplace.
- Records should be stored and carried in a secure bag/case. Records should not be carried ‘loosely’ as this increases the risk of dropping them and losing something.

- Records should be kept separate to laptops and other valuable items to reduce the risk of theft.

It is the responsibility of the staff member to ensure all reasonable precautions are taken to maintain the safeguard of information and they must not be left in the car overnight.

Care must be taken in order that members of the family or visitors to the house cannot gain access to the records. This practice should only occur if the member of staff is not returning to their base after the working day or the records are required for the next working day. Staff must have the agreement of their manager if it is necessary for them to work in this way.

Records should not be away from base for more than one working day i.e. if a member of staff is not returning to base at the conclusion of their working day, the records taken out on visits must be returned on their next normal working day.

There may be exceptional circumstances that mean that this is not possible i.e. if a member of staff goes off sick before returning the notes. In this situation the records should be returned as soon as is practically possible. Managers may have to make arrangements to retrieve records if they are required whilst the member of staff is off for a period of time.

6.5 Tracking records

When an assessment has to be made as to the risk of loss and the loss could compromise patient care or create a serious breach of confidence the following procedure must be followed. The person responsible for sending or taking records must log:

- The name and type of records removed, including any unique identifying number,
- The reason for removal and whether likely to be temporary or permanent if known,
- The date of removal,
- The person the record is being sent / handed over to and method of transfer,
- The date notified that the records have arrived at their destination including name of person confirming receipt, if appropriate.
- The date records return to base, if appropriate.

Where data is received in an insecure manner from another sender recipient should notify the sender and request that any future information must be sent securely.

6.6 Sharing information with other organisations (Non NHS)

Information sharing with non-NHS organisations must be in line with current Data Protection legislation. In all cases, staff should seek approval from the Information Governance Manager before transferring any data. Consideration will also be given as to whether a contractual agreement is required for the transfer.

6.7 Information Sharing Agreement (ISA)

When sharing information with any organisation on a regular basis for a particular purpose, it is good practice to implement an ISA to determine and agree exactly what data will be shared, how the data will be shared and with whom. Please refer to Information Sharing Policy.

6.8 Transferring information outside the UK

There are a number of additional requirements and legal obligations surrounding the transfer of information outside the UK. If any staff have a need to do this, they must seek guidance from the IG Team.

7. Training Required for Compliance with this Policy

All staff to receive Mandatory Information Governance Training on an annual basis.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	Information sharing within and outside of the organisation is carried out securely with adequate protection. Data protection breaches are checked against the information flows.
When will the monitoring be performed?	When incidents occur.
How are you going to monitor?	Incidents reports against the information flows.
What will happen if any shortfalls are identified?	Identify any risks in the information flow.
Where will the results of the monitoring be reported?	Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	Assessment of the risk with the IAO and report back to the working group.
How will learning take place	Recommendations from the working group and identifying any additional training.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Incident Reporting	a) Number of email related incidents. b) Number of internal mail related incidents. c) Number of external mail related incidents. d) Number of SMS related incidents.	System logs for electronic transfer and receipt of paper based transfer documents.	IG Manager.	Information Governance Working Group	When incidents occur and reporting via incident reporting form.	To be determined as a result of the specific findings from each investigation/incident . Supplementary guidance will be issued in the form of Staff Bulletin and the Trust's Intranet.

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with:

- Information Governance Working Group
- Senior Information Risk Owner
- Caldicott Guardian

The policy will be reviewed every three years unless there are significant revisions to be made.

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings

12. References

This document refers to the following guidance, including national and international standards:

- Data Protection Act 1998
- Freedom of Information Act 2000
- NHS Code of Practice: Confidentiality Annex A1 Protect Patient Information
- General Data Protection Regulations 2016
- Data Protection Bill 2018

13. Associated Documentation

This policy refers to the following Trust documents:

- Data Encryption Policy POL-F-IMT-2
- Information Security Policy POL-F-IMT-7
- Internet Policy POL – F – IMT - 9
- Records Management Policy POL-F-IMT-10
- Email Policy POL-F_IMT-12
- Police Request for personal information form FM--O-CCA-1
- Clinical Records Policy POL-CCPS-CQ-2