Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust

Safe Haven Guidelines

This procedural document supersedes: CORP/ITC 8 v.4 – Safe Haven Guidelines

Did you print this document yourself?

Please be advised that the Trust discourages the retention of hard copies of policies (except for emergency authorised hard copy holdings) and can only guarantee that the policy on the Trust website is the most up-to-date version.

Executive Sponsor(s):	Simon Marsh, CIO and SIRO
Name of author/ reviewer: (this version)	Roy Underwood – Data Protection Officer
Date revised:	July 2018
Approved by (Committee/Group):	Information Governance Group
Date of approval:	24 July 2018
Date issued:	13 September 2018
Next review date:	March 2021
Target audience:	All staff, Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 5	13 Sept 2018	• Periodic review • Update to accommodate the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 now commonly known as 'Data Protection Legislation'	Data Protection Officer (DPO)
Version 4	1 April 2015	• Periodic review with changes to Policy Layout and Monitoring arrangements • Change references from CSUs to Care Groups	Head of Information Governance
Version 3	Feb 2012	• Changes to Front Page layout and detail • Complete restructure of the Policy format to meet CQC compliance	Head of Information Governance
Version 2	July 2008	• Changes to Information Governance Toolkit Standard 208 • Changes to reporting authority • Minor changes introducing Bulk Data Transfer arrangements	Head of Information Governance
Version 1	Dec 2006	• Bi-annual review – no changes	Head of Information Governance

Contents

Page No

1 INTRODUCTION

This policy applies to anybody employed or working on behalf of the Trust or who is or maybe involved either directly or indirectly with processing personal and confidential information. The main methods of processing confidential information included within this policy are using the fax, telephone and post: internal and external.

1.1 What is a Safe Haven

A safe haven is a process or place through which confidential information can be received and dispatched securely[1].

1.2 Important Note

It is essential that any activities undertaken in line with this policy are done so in a lawful manner and that personal information is processed, in accordance with current Data Protection Legislation[2].

This policy does not alter any other procedures and practices laid down for staff who deal with confidential information, for instance, Caldicott standards of practice.

2 PURPOSE

Confidential information must not be processed by email unless it is absolutely necessary, i.e. there is no other means of processing that information, as a result limited guidance on the use of email for this purpose is included.[3]

Personal information, whether it be about a patient or a member of staff is fundamental to the provision of an effective NHS. We are all involved with the processing[4] of personal information directly or indirectly during our employment with the NHS and it is our duty to keep this information private and an individual's right for the confidentiality of their information to be respected. For the purposes of this policy, processing refers to the receipt and dispatch of confidential information.

[1] Confidentiality is protected because the information can only be accessed by authorised staff on a "need to know" basis, and the whole process is regulated by a specific set of administrative arrangements, i.e. those identified by this policy or any local procedures introduced by the appropriate head of Department/Division

[2] Please note that GDPR and the Data Protection Act 2018 legislates for both manual and electronic records held about patients and staff.

[3] NHSmail is considered to be a secure medium for transferring confidential information . There are still occasions when 'password protection' should be used, especially when attaching sensitive or personal documents.

[4] Processing refers to how that information is; held, obtained, recorded, used and shared.

2.1 The Principles of a Safe Haven Policy

The underlying principles behind a safe haven policy are, as outlined in the Caldicott and Data Security Reports of 1997, 2013, 2016 and 2017: The basic principles are as follows:

- Justify the purpose
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum information necessary
- Access should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- Consider whether it would be appropriate and lawful to share or not to share

The above principles can be applied to the processing of any personal[5] information, whether it be concerning patients or staff. Sensitive Personal[6] information can only be processed under strict conditions, in most cases requiring the permission of the data subject.

3 DUTIES & RESPONSIBILITIES

Each ***Division/Department*** in their area of responsibility, should ensure that all staff are aware of their responsibilities concerning the handling of confidential information and should ensure that the guidance within this policy is adhered to.

Staff involved in the handling of confidential information have a duty to respect a data subjects rights to confidentiality and to follow the guidance in this policy.

4 RECEIPT OF CONFIDENTIAL INFORMATION

4.1 By Post – External and Internal

Wherever possible, senders of confidential mail into the Trust must be advised of the following procedure

All mail containing confidential information should be sent in a secure and sealed envelope.

Such mail must not be opened by anyone other than the addressee or an appointed deputy, and must be collected personally/or taken directly to the addressee, if internal mail collection and delivery services are not available.

[5] Personal information is that relating to an identified living individual. This can be factual, such as a name, address or date of birth, or it can be an opinion, such as how a manager considers an employee has performed at an appraisal. It can even include an e-mail address.
[6] Sensitive information (defined as 'special category' information under GDPR) includes that relating to someone's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexuality, or criminal proceedings or convictions.

It should be ensured that the addressees NAME and JOB TITLE (in case a post holder leaves before the mail arrives) are legibly PRINTED on the envelope.

4.2 By Telephone

Incoming calls may provoke sensitive/confidential conversation. Exercise caution to ensure sensitive conversations are not overheard. Where a service call is subject to recording, the caller must be informed of that fact.

If the information being given is confidential but irrelevant, the caller should be - sensitively - stopped.

Confidential information given or received over the telephone must be processed appropriately, in accordance with existing standards and/or legislation.

Callers asking for confidential or sensitive information should be questioned, if necessary, as to why they 'need to know'. Ask if you can call them back. Use a number obtained from a valid source, such as the phone book or the CaMIS PAS. Remember you may be speaking to a close relative rather than the patient themselves - try to be helpful, provided you are sure that the caller has a 'right to know'?? If you are in any doubt, pass the call or enquiry on to a senior manager.

4.3 By Fax

Comprehensive guidelines for use of Fax machines are attached at Appendix 2.

4.4 By Email

Before you open an email with an obvious privacy marking, ask yourself, "am I the intended recipient?". If you think that you are not, then please advise the sender, and take action as per the senders footnote - if there is one - you will probably be asked to delete the eMail, if in doubt, ask the sender.

Afford the content of any incoming eMail the same and appropriate degree of privacy and confidentiality[7] with which it is 'marked', whilst you are processing[8] it, whether that content is saved on a computer system or saved as a hard copy.

[7] Doncaster District Information Sharing Policy
[8] Data Protection Legislation

5 DISPATCH OF CONFIDENTIAL INFORMATION

5.1 By Post – External and Internal

External mail (where it contains 'personal data'[9]) may be subject to the Trust's Bulk Data Transfer Guidelines (BDT) – ref CORP/ICT 20. Envelopes must be sealed and addressed in the same way as is the case for incoming mail.

Confirm the recipient's address if you are in any doubt. Staff should consider contacting those to whom they are sending confidential information, to ensure that the correctly-marked envelope (with address for returning if undelivered) will be sent to a specific post-holder at a specific location. Remember that the more concise and correct the information you provide is, then, the more chance there is of successful and problem free delivery.

5.2 By Telephone

Confidential information should only be given if disclosure is to an authorised source and it is known exactly why it is required. If you are in any doubt as to the recipient's identity or their reasons for wanting the information, then you should offer to ring the recipient/caller back. It should always be confirmed that the information is being given to a safe-haven area, for instance that any information processed as a result of the call is being processed confidentially.[10/11]

5.3 By Fax

Comprehensive guidelines for use of Fax machines are attached at Appendix 2.

5.4 By Email

Confidential information can only be sent by eMail using NHSnet to NHSnet addresses (e.g.: jo.bloggs@nhs.net ← → fred.flintstone@nhs.net) as expressed by the Caldicott Guardian, where all Risk issues have been considered. NHSnet is encrypted end-to-end automatically, the User does not have to do anything. Where you need to attach a sensitive or private document, you should consider password-protecting[12] the attachment. This password must be issued separately from the email, either via the telephone or by post. Please also take advise from the Trust eMail Policy CORP/ICT 27, as in some cases transmitted patient data may need to be printed off and included in the patients notes. NHS Mail is a messaging system and is NOT a data strorage platform.

Confirm the email address of the recipient and the spelling of any awkward words or names.

[9] Durant v FSA
[10] Information Sharing Policies
[11] Data Protection Act 2018
[12] Microsoft products include minimal password protection facilities, but you should use WinZip wherever possible.

Check with the intended recipient that the mailbox you are sending to adheres to the principles of a safe haven, i.e. that it is only accessed by those authorised to view such information.

Confidential or sensitive information should not be sent to shared or group eMail boxes unless you are completely sure of the group members and their security arrangements.

If there is regular confidential/sensitive traffic between trust Users, then you should consider the use of a 'User defined' network folder, then you only have to alert colleagues that they need to go there.

Clearly state in the subject window: "CONFIDENTIAL"

Ensure that your email contains a disclaimer[13] such as the one below.

6 TRANSFERRING CONFIDENTIAL INFORMATION OUTSIDE OF THE METHODS DESCRIBED ABOVE

Should it be necessary to move written or disk-based 'Confidential' information between offices then it must be placed in a sealed envelope by an authorised person and transferred either by that person, another authorised person or by a person nominated by an authorised member of staff.

Any Bulk Data Transfer of personal data (manual or electronic) must be authorised[14], and compliant with the Trust BDT policy.

7 OPERATION OF THE POLICY AT ALL OTHER SITES WHERE TRUST STAFF OPERATE

The Guidelines should be adapted where appropriate, for use on other sites where Trust staff operate, taking into account local circumstances.

Local managers will organise the operation of the Guidelines on all their sites in what they see as being the most suitable way.

[13] **FOI & CONFIDENTIALITY STATEMENT**

The information contained in this eMail may be subject to Public Disclosure under the NHS Code of Openness, or the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this eMail and your reply cannot be guaranteed.

This eMail and any files transmitted with it are confidential. If you are not the intended recipient, any reading, printing, storage, disclosure or copying or any other action taken in respect of this eMail is prohibited and may be unlawful. If you are not the intended recipient, please notify me immediately by using the reply function and then permanently delete what you have received. Thank you for your cooperation.

[14] Authorisation for BDT of patient or staff personal data is the responsibility of the Caldicott Guardian or an appointed deputy

8 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

Safe Haven locations will be subject to unannounced and periodic inspection by the Head of Information Governance/DPO.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Staff do not leave files/computer terminals unattended/unsecured. Staff double check to avoid transmitting information to the wrong person or fax machine[15] Staff do not allow sensitive conversations to be overheard. Staff guard against people seeking information by deception. Staff Log out or Lock their screen down when leaving their desk for any length of time.	The Trust Information Governance Group – Secret Shoppers	One area per month and in line with IG Toolkit standards	To the IG Group in line with Data Security & Protection (DSP) Toolkit standards

9 EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment for All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 3).

10 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/EMP 4 – Fair Treatment for All Policy
CORP/EMP 27 – Fair Treatment for All Policy
CORP/ICT 3 – Information Management Systems (Registration) Policy
CORP/ICT 7 – Data Protection Policy
CORP/ICT 20 – Bulk Data Transfer Guidelines

11 DEFINITIONS

Not applicable.

12 REFERENCES

Not applicable.

[15] Safe Haven Guidelines: CORP/ICT 8

APPENDIX 1 - SAFE HAVEN AUDIT/CHECK LIST

	Yes/No	Action required	Target Date
Do you have a Safe-Haven Co-ordinator or someone in a similar position?			
Have you identified the location of your Safe-Haven/s?			
Are Staff authorised to handle confidential information within each Safe-Haven?			
Do you take account of changes in post holders or other Safe-Haven conditions?			
Do you have procedures/guidelines for the receipt of confidential Information by the Trust?			
Do you have procedures/guidelines for the dispatch of confidential information from the Trust?			
Do you have procedures/guidelines for the transferring confidential information outside of the methods described above?			
Do you have working arrangements within the Safe-Havens?			
Do you have the same or similar procedures/guidelines for the operation of the policy at all other sites?			
If you hold personal data records are they notifiable to the Caldicott Guardian? CORP/ICT 3 Refers			

This audit/check list is intended as a guide towards the sorts of questions you may need to ask and answer - it is not exhaustive

APPENDIX 2 - GUIDELINES FOR THE SECURE TRANSMISSION OF MANUAL FAXES

The Health Service holds large amounts of confidential information about you, members of your family, friends, and colleagues; but the vast majority of this information is about strangers you are probably unlikely to meet. The information is about them but it actually belongs to Secretary of State for Health and we are merely the custodians. Their information should be treated with as much respect and integrity as you would like others to treat your own information. Handle with care; it is your responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that patient identifiable or sensitive trust information is not made available to unauthorised persons.

One of the most common breaches of confidentiality occurs when documents containing patient identifiable information are sent by fax machine. It is our mission to minimize the number of Fax machines in use, so you should consider carefully whether there is a safer alternative, or indeed whether you actually need a fax machine at all. That said, the fax machine you are sending your information to could be sited in an open office or even in a corridor, and may be shared by more than one department; thereby increasing the risk of the information being seen by unauthorised persons. It is the senders responsibility to ensure that the Fax machine they are using and indeed the recipients fax machine meet Safe haven Guidelines.

Whilst these guidelines deal with patient identifiable information, the procedure is also applicable when faxing any document that contains confidential or trust sensitive information.

What is patient identifiable information?

Patient identifiable information is any collection of the items listed below which could give rise to the positive identification of a living individual:

- Surname
- Initials
- Date of birth
- Post code
- Sex
- National Insurance Number
- Telephone number
- National & Local identifiers (e.g. NHS, Hospital or GP Practice Number)
- Forename
- Address
- Other dates (e.g. death, diagnosis)
- Occupation
- NHS number
- Ethnic group

Many NHS organisations are adopting the principle of Safe Haven fax machines and you should make every effort to ensure you use them wherever possible.

What is a Safe Haven fax machine?

A Safe Haven fax is managed in such a way that you can be confident that information can be transferred to it in the knowledge that safeguards in place to ensure its security. These safeguards may include:

- The fax machine being sited in a secure room or cupboard
- Organisations have a written policy or guidelines for handling faxes that staff have been informed about and understand, and
- Staff who are responsible for collecting and delivering the faxed information to the appropriate person are trusted and have signed up to the Trust's Confidentiality - Code of Conduct through their contracted employment conditions[16].

How do I know if the fax machine I am sending information to is a Safe Haven fax machine?

Telephone the recipient first if you are in doubt regarding the security of their fax machine.

What sort of information do I need to know to ascertain whether or not it is a Safe Haven fax machine?

You could ask simple questions, for example:

i. Is the fax machine sited in a secure office?
ii. Does more than one department use the fax machine?
iii. Are there designated people who collect faxes?

What shall I do if the fax machine is not a Safe Haven fax machine?

- Telephone the recipient of the fax (or their representative) to let them know you are going to send patient identifiable information by fax.
- Ask if they could wait by the fax machine whilst you send your message through.
- Ask if they could acknowledge receipt of the fax.
- Make sure you use a fax cover sheet that states that the information you are sending is confidential *** Please see below for a suggested form of words**

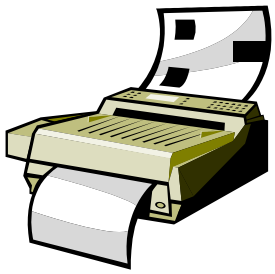
***** The information contained in this fax is **STRICTLY CONFIDENTIAL** and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately. Thank you.

[16] **INFORMATION GOVERNANCE.** The Trust requires its employees to comply with all aspects of Common Law (UK), the Data Protection Act 2018, GDPR, the Computer Misuse Act 1990, and other Lawful enactments and related Trust Policies that are concerned with the processing of the trust's personal and/or sensitive information assets. The Trust expects its employees to maintain the confidentiality, quality and integrity of those trust sensitive and personal information assets with which they come into contact in the course of their employment. Any unauthorised or inappropriate disclosure or use of information may be treated as a serious breach of discipline, possibly leading to dismissal. You should consult with your Line Manager in case of doubt.

- Double check the fax number before you hit the “send” button to ensure that the correct number has been dialed.
- Request a report sheet to confirm that transmission is OK
- If it is a number that is used regularly, it can be stored in the fax memory. Once stored, you could send a test fax with NO sensitive data for added confidence and ask the recipient to do the same for you.

Other safeguards for secure transmission of confidential information

It is NOT advisable to:



- send faxes to a destination where you know they are not going to be seen for some time.
- send faxes to a destination outside office opening times (whenever possible).
- leave the information unattended whilst the information is being transmitted.

If you find a confidential document has been sent to your fax machine in error, it is your responsibility to ensure it is given to the named recipient or securely returned to its source.

This guidance also covers personal information about staff as well as patients.

If your organisation has a Safe Haven fax machine(s), make sure you pass the number(s) on to your colleagues who regularly send confidential information to you.

Remember, if in doubt – check it out!

Take care of personal information – it could be yours

APPENDIX 3 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	CSU/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Safe Haven Guidelines	IM&T	Data Protection Officer	Existing Policy	06/07/2018

1) Who is responsible for this policy? Name of Care Group/Directorate: IM&T

2) Describe the purpose of the service / function / policy / project/ strategy? To ensure that information coming onto and going out of the Trust is kept safe

3) Are there any associated objectives? Data Protection Act 2018/GDPR/NHS Digital Code of Practice for Records Management

4) What factors contribute or detract from achieving intended outcomes? Information Governance (SET) Training & Education

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? NO

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) Is there any scope for new measures which would promote equality? NO

7) Are any of the following groups adversely affected by the policy?

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: March 2021

Checked by: Data Protection Officer **Date:** 06/07/2018