London Ambulance Service NHS Trust

Safe Haven Policy and Procedure

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This document aims to increase staff awareness around the secure transmission of personal information and to advise staff on how to manage areas processing personal information as a Safe Haven.

Sponsor Department: IM&T Information Security

Author/Reviewer: Information Security Manager. To be reviewed by August 2016.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
02/10/2013	2.1	Information Security Manager	Amendments as advised by SMT
23/07/2013	1.2	IG Manager	Further amendments and new Implementation Plan
26/06/2013	1.1	Information Security Manager	Review and amendments
07/07/2010	0.6	Information Security Project Manager	Final amendments for submission
06/07/2010	0.5	Head of Records	Further amendments
02/07/2010	0.4	Records Manager	Re-format
21/05/2010	0.3	Head of Management Information	Draft amendments
16/05/2010	0.2	Operational Information & Archives Manager	Draft amendments
24/03/2010	0.1	Information Security Manager	Initial Draft

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
SMT	28/08/13	2.0
SMG	14/07/10	1.0
Ratified by (If appropriate):		

Published on:	**Date**	**By**	**Dept**
The Pulse (v2.1)	08/10/13	Governance Co-ordinator	GCT
The Pulse	27/07/10	Records Manager	GCT
LAS Website (v2.1)	08/10/13	Governance Co-ordinator	GCT
LAS Website	27/07/10	Records Manager	GCT

Announced on:	Date	By	Dept
The RIB	08/10/13	IG Manager	GCT
The RIB	03/08/10	Records Manager	GCT

EqIA completed on	By
05/07/10	Head of MI, Information Security Manager, and Head of Records Management
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
	Principles of Information Security - NHS Connecting for Health (http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security)	
	Information Security Technology Techniques – Information Security Management System Requirements 27001: 2005 – British Standards Organisation	
	Data Protection Act 1998	
	Common Law Duty of Confidence	
	NHS Code of Practice: Confidentiality	
TP/009	Policy for Access to Health Records, Disclosure of Patient Information, Protection and Use of Patient Information	3.0
TP/012	Data Protection Policy	3.1
TP/047	Electronic Information Handling Procedure	2.1

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are neither controlled nor substantive.

1. Introduction

In order to be able to provide an effective ambulance service, the London Ambulance Service NHS Trust (LAS) routinely processes personal information. The way in which this personal data is handled needs to be managed in a way that ensures acceptable levels of confidentiality.

The information the Trust processes is not the property of the Trust. It belongs to the people that it is collected from. The Trust acts as a custodian of the data and as such is responsible for the safe keeping and security of the data.

Whilst the Trust holds this information, all staff that have access to this data must ensure that they do everything possible to protect this information from those that are not authorised to use it or view it. This is enforced through the Caldicott Principles and the requirements of the Data Protection Act, 1998.

This document outlines the policy and procedure to follow whilst transferring such data both within the Trust and to external recipients and when other agencies or Trusts want to send such data to the Trust to ensure that the data is handled appropriately. The way in which this must occur is known as a safe haven procedure. Personal and sensitive data (e.g. individual's medical records) need to be transferred between safe havens (see section 5.2 for details of what makes an area a safe haven).

2. Scope

This policy covers the handling of confidential and sensitive patient information and applies to all permanent and temporary staff as well as third parties acting on behalf of the Trust.

3. Objectives

The objectives of this policy are to:

1. Ensure that the confidentiality and security of personal information held by the Trust is maintained at an acceptable level. This includes when Trust data is sent to third parties and other partner organisations.

2. Ensure that staff are aware that all routine information flows of personal information both internally and externally must be notified to the Information Security department, risk assessed and recorded within the corporate information flow map.

3. Ensure all staff and third parties understand their responsibilities in managing patient confidentiality.

4. Ensure that all staff and third parties understand what a safe haven is and how to manage their work areas as a safe haven.

4. Responsibilities

4.1 Medical Director

Responsible for ensuring that all personal data received is managed in accordance with the Caldicott Principles and ensuring that this document meets the Caldicott Principles. The Medical Director acts as the Trust's Caldicott Guardian with responsibility for patient confidentiality.

4.2 Senior Information Risk Manager (SIRO)

Responsible for ensuring that all risks to information are identified and managed effectively in line with relevant legislation.

4.3 Head of Infrastructure

Responsible for ensuring that communication devices are configured in line with this policy and procedure.

4.4 Information Security Manager

Responsible for reviewing and risk assessing safe havens and associated procedures for adequacy to ensure they meet Caldicott and Data Protection Act, 1998 requirements.

4.5 Information Governance Manager

Responsible for data protection matters and information management arrangements are in place to allow for the process laid out within this policy and procedure.

4.6 Line Managers

Responsible for ensuring staff work in line with these safe haven arrangements at all times.

4.7 All Staff and Third Parties

Responsible for ensuring that any processing of person identifiable information is in line with this policy and that all safe haven arrangements are followed.

5. Definitions

5.1 Safe Haven

A safe haven is a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the Trust to

ensure confidential personal information is communicated safely and securely. It is a safeguard for sensitive personal information which enters or leaves the Trust whether this is by fax, post or other means. Any members of staff handling sensitive personal information, whether paper based or electronic, must adhere to the safe haven principles.

5.2 Personal Information

As per the Data Protection Act, 1998, personal information is information that can be used to identify a living individual. This might be fairly explicit such as an unusual surname or isolated postcode or a collection of different information that 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.

5.3 Sensitive Personal Information

As per the Data Protection Act, 1998, sensitive personal information is a category of personal information whose unauthorised disclosure could impact adversely on an individual. This is defined as information about individuals concerning:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Trade union membership
- Physical or mental health condition
- Sexual life
- The commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed including the sentence terms of any court.

For this type of information even more stringent measures should be employed to ensure that the data remains secure and that the individual's information is adequately protected.

5.4 Processing

Any activity that can be carried out on personal data.

5.5 Data Controller

Any person who controls the processing of personal data.

5.6 Data Subject

The individual person who is the subject of any relevant personal data.

5.7 Information Flow

Data that is routinely transferred internally or with third parties is an information flow. Information flows can be inbound or outbound or both.

6. Where Safe Haven procedures should be in place

Safe haven procedures should be in place in any location where large amounts of personal information is being received held or communicated (e.g. mail rooms) especially where the personal information is of a sensitive nature such as patient-identifiable information. There should be at least one area designated as a safe haven at each of the Trust sites where personal information is processed.

7. Requirements for Safe Havens

7.1 Physical security and location

7.1.1 It should be a room that is locked or accessible via a coded key pad known only to authorised staff; or

7.1.2 Where possible, the office or workspace should be sited in such a way that only authorised staff can enter that location e.g. 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;

7.1.3 The office should allow for adequate storage for sensitive material, including waste, whilst waiting for collection;

7.1.4 If sited on the ground floor any windows should have locks on them;

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

7.1.6 Manual paper records containing person-identifiable information should be stored in locked cabinets;

7.1.7 Computers should not be left on view or accessible to unauthorised staff and have a secure screen saver function and be locked or switched off when not in use;

8. Communications by fax

8.1. Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules apply:

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- Faxes should always be addressed to named recipients.
- Always check the telephone number to avoid misdialling and ring the recipient to check that they have received the fax. If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.
- You notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- Faxes containing sensitive personal data are not left lying around for unauthorised staff to see.
- Remove patient identifiable data from any faxes unless you are faxing to a known safe haven. Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier used such as CAD reference.
- Faxes sent should include a cover sheet, which contains a suitable confidentiality clause (see appendix 1).
- A fax machine used to receive person identifiable or sensitive information must be located in a secure environment. Faxes should be removed from the machine on receipt. The sender should be contacted to confirm receipt and the fax appropriately dealt with and safely stored.

8.2 If the organisation that you need to fax does not have a Safe Haven fax machine, then follow the rules below:

DO …

- Telephone the recipient of the fax to let them know that you are about to send a fax containing confidential information.
- Ask if they will wait by the fax machine whilst you send the document.
- Ask if they will acknowledge the receipt of the fax.
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential.

- Please see Appendix 1 for a fax confidentiality clause.
- Check the fax number you have dialled and check again that it is correct before sending.
- Request a report sheet to confirm that the transmission was sent correctly.
- If this fax machine is going to be used regularly, consider storing the number in your fax machine's memory.

DO NOT…

- Send faxes to where you know that the information will not be seen for a period of time.
- Send faxes at times that maybe outside the recipient's hours of work
- Leave information unattended whilst a fax is being transmitted

8.2 If you receive confidential information on your fax machine, it is your responsibility to inform the sender that you have received this information.

9. Communications by Post

9.1 All sensitive personal records must be stored face down in public areas and not left unsupervised at any time.

9.2 Incoming mail should be opened away from public areas.

9.3 Outgoing (both internal and external) written communications or mail containing personal information should be transferred in a sealed envelope and addressed to a named recipient. They should be clearly marked "Personal and Confidential - to be opened by the recipient only". This means personal information should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, unit or organisation. In cases where the mail is for a department it should be addressed to an agreed post holder or department manager.

9.4 Special care should be taken with personal information sent in quantity, such as case notes, or collections of patient records on paper. Electronic media must always be encrypted, refer to TP/047: Electronic Information Handling Procedure for instructions. Items should be sent by Recorded Delivery or by Trust courier if the data contains personal information about 51 or more individuals, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

9.5 The recipient should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.

9.6 The personal information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.

9.7 If the internal mail system is being used for person identifiable or sensitive information, it is essential that physical security measures, such as key coded or swipe card entry, are in place to protect information in the post-room, post collection point or similar.

10. Communications by Email

10.1 Emails containing person identifiable or sensitive information must be stored appropriately on receipt, e.g. incorporated within the health record, and deleted from the email system when no longer needed.

10.2 NHSmail (user@nhs.net) is the only approved email service for securely exchanging personal identifiable data between NHS trusts. Therefore the lond-amb.nhs.uk email must not be used for sending confidential information.

Both the sender and recipient need to use NHSmail or other secure encrypted email systems for the information to be adequately protected.

10.3 All personal information sent by e-mail should be sent to a named individual.

10.4 Personal information of a more sensitive nature should be sent over NHSmail with appropriate safeguards:

- Clinical information is clearly marked;
- Emails are sent to the right people;
- Browsers are safely set up so that for example, passwords are not saved and temporary internet files are deleted on exit;
- The receiver is ready to handle the information in the right way;
- 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 not Trust property.

10.5 Transfer of personal information by Trust Outlook email (lond-amb.nhs.uk) must be avoided unless the information is encrypted. Password protected files are not sufficient protection and must not be used as a substitute for encryption.

10.6 Internet based email systems such as Hotmail must never be used to transfer Trust information.

10.7 Please also refer to TP/047: Electronic Information Handling Procedure for specific guidance on sending personal information electronically.

11. Communications by Telephone

11.1 Recorded telephone messages containing person identifiable or sensitive information, e.g. the names and addresses of applicants phoning for a job, or patient details, must be received into a secured, password protected voicemail box, so that only those entitled to listen to the message may do so.

11.2 The Infrastructure department will ensure that a password is required to gain access to messages.

11.3 Some departments use a messages book to note messages for absent staff members. This should also be stored securely.

11.4 If information is to be shared by telephone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant phone number, double checking that it is the correct number for that individual / organisation and then calling the recipient back.

11.5 Where information is transferred by phone, care should be taken to ensure that personal details are not overheard by other staff that do not have a “need to know”. Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts etc.

11.6 Messages containing personal information should not be left on answer machines unless a password is required to access them. They should also not be stored on communal systems.

12. Use of Computers

12.1 Access to any electronic device that can access sensitive personal data must be password protected. No passwords or accounts are to be shared.

12.2 Device screens, including devices in ambulances, 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 can see personal data. Devices not in use should be switched off locked or have a secure screen saver in use.

12.3 Information should be held on the Trust's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.

13. Verbal and other communication

13.1 A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality particularly in modern open plan offices. Care should be taken to ensure that confidentiality is maintained in such discussions.

13.2 Messages containing confidential / sensitive information should not be written on white boards / notice boards.

14. Sharing personal information internally and within the NHS

14.1 Staff who share personal information routinely (e.g. regularly), which includes both sending and receiving data, are creating information flows. All information flows must be reported to the Information Security Department for inclusion in the Trust Information Asset Register. A local Information Asset Owner needs to be identified as the owner of this data flow and a risk assessment carried out to ensure that adequate controls are in place.

14.2 For further advice please contact the Information Governance Manager or Information Security Manager.

14.3 A formal Information Sharing Agreement should be put in place if sharing bulk or routine personal information for secondary use purposes between NHS trusts. Please contact the Information Governance Manager for the template and advice.

15. Sharing personal information with other organisations (Non NHS)

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

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

- Data Protection Act 1998
- Common Law Duty of Confidence
- NHS Code of Practice: Confidentiality

15.3 An Information Sharing or contractual agreement must be put in place if there is a requirement to share or transfer bulk or routine personal information between the LAS and any other organisation.

16. Policy Exceptions

16.1 Any exceptions to this policy must be formally requested to the Information Security Manager for consideration. If it is felt that you cannot meet the criteria laid out within this policy, please speak to the Information Security department.

17. Reporting Breaches

17.1 Any breaches of this Policy must be reported immediately via the IM&T Service Desk or, out of hours to the On-duty Manager. They will escalate the issue appropriately depending upon the severity of the incident.

IMPLEMENTATION PLAN				
Intended Audience	All LAS Staff			
Dissemination	Available to all staff on the Pulse and to the public on the LAS website.			
Communications	Revised Policy and Procedure to be announced in the RIB and a link provided to the document.			
Training	Training will be provided as part of the Information Governance awareness programme			
Monitoring:				
Aspect to be monitored	**Frequency of monitoring AND Tool used**	**Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported**	**Committee/ group responsible for monitoring outcomes/ recommendations**	**How learning will take place**
Compliance will be checked through incident monitoring	6 monthly Safe Haven review	The Information Security manager will report results to the Information Governance Group	Risk Compliance and Assurance Group	Dissemination of findings and action to be taken where change to practice is required

London Ambulance Service NHS
NHS Trust

Appendix 1
LA063

Fax: Confidentiality Clause

Station/Department/Unit Name
Headquarters
220 Waterloo Road
London
SE1 8SD

Tel: 020 1234 5678
Fax: 020 1234 5678

To:		**Fax:**	*fax number*
From:	*Department name*	**Date:**	
Organisation		**Pages:**	*Number of pages including this*

Please quote reference _____/___/_____ N^{o} in all enquiries.

Comments:

The information contained in this fax is confidential and should not be copied, distributed or disclosed. If this fax has been received in error, please dispose of this as confidential waste.

Thank you for your assistance.