London Ambulance Service NHS Trust

Electronic Information Handling Procedure

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This document concerns the management of information and includes statements on the secure creation, storage, transfer/transmission and destruction of data.

Sponsor Department: IM&T Information Security

Author/Reviewer: Information Security Manager. To be reviewed by Feb 2012.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
09/03/09	1.1	Records Manager	reformatted ratified document to bring in-line with corporate style
28/01/09	0.6	Information Security Manager	Removal of paragraphs / minor changes.
03/01/09	0.5	Head of Records Management / Information Security Manager	amendments / IGG amendments
29/08/08	0.4	Information Security Manager	Updated secure transfer process after IGG and CfH consultation
14/08/08	0.3	Information Security Manager	Removed references to paper based information
04/08/08	0.2	Head of Records Management/ Information Security Manager	Draft amendments and structuring
11/07/08	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**
Information Governance Group	03/02/09	1.0
Ratified by:		
RCAG	16/02/09	1.0

Published on:	Date	By	Dept
The Pulse	09/03/09	Records Manager	GDU
Website	11/03/10	Records Manager	GDU

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**

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 not controlled nor substantive.

1. Introduction

The London Ambulance Service NHS Trust (LAS) has a responsibility to ensure that electronic information is used securely. This is to be achieved through the use of physical and software controls.

This document concerns the management of information and includes statements on the secure creation, storage, transfer/transmission and destruction of data.

2. Objective

To prevent unauthorised disclosure, modification, removal or destruction of LAS electronic information assets and disruption to LAS business activities

.

3. Scope

All electronic information systems owned or operated by or on behalf of the LAS.

4. Procedure

4.1 Responsibilities

IM&T Director

- Responsible for ensuring that electronic information is managed effectively and securely throughout the Trust.
- Responsible for ensuring that the LAS has appropriate data encryption capabilities in order to protect data that is processed on removable media.

Directors

- Must authorise the export of any bulk extracts of confidential or sensitive data for their work areas.
- May delegate this authorisation as appropriate.

Information Security Manager

- Should identify and implement any configuration requirements required to comply with NHS Information Governance security policy and standards. This includes data encryption capabilities.
- Is responsible for assuring that the data encryption functionality and procedures used with removable media have been implemented correctly, are of appropriate strength and fit for purpose.
- Is responsible for producing and reviewing this procedure

Managers

- Are responsible for ensuring their staff are aware of and abide by this procedure.
- Are responsible for the day-to-day management and oversight of electronic information used within their work areas to ensure this procedure is followed.
- Are responsible for managing any 3rd party activity within their work area to ensure that the requirements in this procedure are adhered to.
- Managers must ensure that removable media is returned to the Information Security Manager if staff leave.

Employees and contractors/Internal 3rd parties

- Must not use any electronic information systems or removable media other than those provided or explicitly approved for use by IM&T.
- Are responsible for ensuring that all sensitive data stored on removable media (such as laptops) used to store sensitive data is encrypted.
- Must always manage information securely.

External 3rd parties

- Must use any data supplied by the Trust in a secure manner and abide by an agreed information sharing agreement which would be drafted in line with the broad principles of the Information Security Policy.
- Will be responsible for ensuring the security of any data supplied by the Trust.

4.2 Removable Media – storage and transmission of data

4.2.1 The use of removable media by sub-contractors or temporary workers must be specifically authorized by the contract/line manager for an identified and agreed business need.

4.2.2 IM&T will identify removable media that has been approved for use within the LAS.

4.2.3 Removable media may only be used to store and share LAS information that is required for a specific business purpose.

4.2.4 Removable media used to store patient identifiable or sensitive information must be encrypted as per the Information Security Policy and associated procedures.

5.2.5 When the information stored on removable media is no longer required for the business it will be removed through a destruction method that makes recovery of the data impossible. Alternatively the removable media should be destroyed beyond its potential reuse. In all cases, a record of the action to remove data or to destroy data should be recorded in an auditable log file.

4.2.6 Removable media must be returned to IM&T when a staff member leaves the LAS.

4.2.7 Removable media must be physically protected against loss, damage, abuse or misuse when used, where stored and in transit. The owner must also ensure that sensitive data is encrypted and must take responsibility for security of their data whenever it is taken off site.

4.2.8 Data archives taken and stored on removable media, either short-term or long-term, must take account of any manufacturer's specification or guarantee and any limitations therein.

4.2.9 IM&T will provide guidance on effective storage times of removable media to all staff when new equipment is issued and on demand (see Appendix 1).

4.2.10 Loss or misuse of removable media must be reported to the Information Security Manager immediately and in accordance with the LAS Incident Reporting Procedure.

4.3 Removable media: Data Encryption Procedure

4.3.1 All removable media will be encrypted and the Information Security Manager will ensure that:

- only e-gif approved encryption algorithms should be used to encrypt and protect relevant LAS data. (See e-gif technical standards)
- only currently approved cryptographic algorithms are used for encryption – these are 3DES, AES, AES (FIPS 197) and Blowfish which should be used at a minimum of 256bit strength.
- The use of freeware or shareware that does not benefit from independent security evaluation or that fails to comply with these standards is not permitted and must be avoided.

4.3.2 The Information Security Manager will decide whether encrypted files will be created on removable media. Where the data is to be encrypted, an encrypted file may be created on the removable media through the application used for processing where this contains relevant encryption capability (or) through the use of an additional security product with this encryption functionality. Such products may include ones that can be used to create self-decrypting archives (SDAs) and others that encrypt data files automatically when copied to removable media.

4.3.3 The pass-phrase or decryption key used for encryption/decryption purposes must be sufficiently long and complex to prevent the encrypted information from attack. The decryption pass-phrase or key must never be sent with encrypted removable media.

4.3.4 All incidents involving encrypted data must be reported to the Information Security Manager immediately and in accordance with the LAS incident reporting procedure.

4.4 Physical Media in Transit

4.4.1 The Trust appreciates that information needs to be exchanged in order for the Trust to support the business on a day to day basis. However, any information exchanged needs to be carried out in a secure manner. Note that judgement may be made to work outside the following categories where circumstances dictate.

Data may be transferred by post/courier as laid out in the following sections.

4.4.2 Standard Post

Suitable for the transfer of:

1. person identifiable data concerning a single individual;
2. information that poses minimal risk if the data is lost;
3. person identifiable data concerning more than one individual that has been sufficiently redacted to the point that no single individual can be identified;
4. correspondence sent as part of your working life.

4.4.3 Registered (Special Delivery) Post

Suitable for the transfer of:

1. person identifiable data about one person that is deemed highly sensitive or if unauthorised disclosure could result in significant harm or distress to an individual;
2. person identifiable data that contains information about more than 5 and less than 20 individuals;
3. sensitive information that could damage any ongoing contractual obligations or relationships with 3rd parties if the data were to be disclosed in an unauthorised manner. This includes information that could damage any ongoing negotiations with any 3rd parties.

4.4.4 Secure Courier

Suitable for the transfer of:

1. person identifiable data that contains information about 20 or more individuals;
2. highly sensitive data where unauthorised disclosure could cause the Trust significant damage to its reputation and/or prolonged media interest;
3. highly sensitive data that could cause endangerment to a large number of individuals and/or wide scale damage to its reputation or loss.

The process for use of secure couriers is as follows:

1. Authority to dispatch information is received by relevant Director. Subsequent authority to use courier service is obtained from Line Managers.

2. A signature sheet is used to capture details of handover/takeover of the data disks. Packaging is checked to ensure it is sufficient to protect the contents from physical damage.

3. The identification of courier is checked before handover of media. The sender signs the courier's signature sheet.

4. A telephone call to notify despatch is made from the despatching organisation to a named individual in the receiving organisation.

5. Nominated staff at the destination receive the disks and sign the courier's signature sheet. The recipient then notifies sender who supplies the pass-phrase via telephone.

6. The disks or other media are to be destroyed by the receiving party by cross cut shredding or secure disposal.

4.4.5 The Trust will also handle protectively marked documents from 3rd parties as part of normal business. Any such information must be handled as per guidance supplied by the authoring or supplying body. If there is any doubt as to how to appropriately transfer any protectively marked data, please contact the Information Security department for advice.

4.5 Use of Email

4.5.1 **Secure email process** - For transfer of person identifiable or sensitive information

- NHS Mail must be used to transfer person identifiable or sensitive information to other NHS Trusts or third parties with a valid NHS Mail account where possible.

- If LAS supplied Outlook or Outlook Web Access is to be used to transfer sensitive or person identifiable information, appropriate encryption must be employed. In the first instance, contact the Information Security Manager for advice.

If data is sent by email, the decryption key must be provided by telephone or other method. The pass-phrase or decryption key used for encryption/ decryption purposes must be sufficiently long and complex to prevent the encrypted information from attack.

- Under no circumstances must any pass phrase or key used for encryption be sent over email to any recipients.
- Upon receipt, the recipient must notify the sender.

4.6 Data Removal

It is important to maintain an effective method of managing the process of data removal and destruction. This ensures that all media requiring clearing or destruction is correctly organised and properly audited.

Clearing and purging must be used for the removal of data.

4.6.1 Clearing

If the disk drives/media will remain within the same environment, in which they are currently situated (and existing security measures will continue to cover them), the most appropriate removal method is clearing.

As long as particular sections of data need removing and comprehensive data removal from the media is not required, then any LAS staff or contractors may carry out clearing.

Approved clearing programs must be used to write at least three sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs.

To ensure that historical data is thoroughly removed it is advisable to make as many passes as is practicable. The likelihood of total data eradication is proportional to the amount of passes.

4.6.2 Purging

Purging is required when media moves from an existing security zone to a new security zone. This new zone may or may not be more secure than the current security measures in effect.
After removal of media from its current security context there must be sufficient care taken to ensure that data is irretrievable, even if specialised methods are used such as secure disposal through approved third parties.

Purging involves the use of more sophisticated tools and therefore requires IM&T staff working within a controlled environment.

Purging of media must involve a minimum of seven passes to qualify as an acceptable purging process.

4.6.3 Data Removal from Live Systems

There are various scenarios in which data may need removing from a system while still in operation, or reuse of the media is required for financial or policy reasons. This includes data removal from hard disks or tape backup devices, when a particular application or the LAS no longer requires it.
In such cases, all staff and contractors must make all possible efforts to remove the required data from the target media without adversely affecting the performance of live systems or the long-term effectiveness of the media to perform the role required of it.

4.6.4 Data Removal for Media Reuse

If media such as hard disk drives are reused rather than completely decommissioned clearing must be employed if the media will remain within the same security zone.
If media is to be used in another security zone, purging must be employed.

A log of all clearing and purging processes (for each media drive) must be kept to provide an audit trail that records all the areas that the media has been in use and, before reuse of the media in a different area, the verification of data removal.

Unless there is a compelling business reason to do so, media should not transfer between differing security zones.

4.6.5 Verification of Data Removal

Once a specialist company, contractor or IM&T staff member has processed the media, there should be a procedure for verification of data removal, including the issuing of certificates.

If IM&T staff or specialist third parties have carried out the data removal then the process should be recorded (along with the verification results) and stored with all other relevant documentation.

Tools that attempt to retrieve data from media (which has undergone a data removal process) may be used to verify that complete data removal has taken place. If any files or fragments of files are evident, then data removal has been unsuccessful. If so, contact the Information Security Manager for advice.

4.6.6 Media Log

Use of inventory tracking software may be used to minimise the overhead of management. Tracking of hard disk serial numbers at a minimum should be used for individual component tracking.

The log should also contain a section for destruction or removal certificates; these provide evidence guaranteeing the destruction or sanitisation of the media and the date on which the destruction occurred.

4.7 Disposal of Media

4.7.1 General

Line Managers are responsible for ensuring that CDs and DVDs that are no longer required are shredded, either by the use of provided secure waste disposal arrangements or by the use of a cross cut shredder locally and disposal of any shredded media as secure waste. This must occur in line with the secure waste procedure.

All other media, which is no longer required (or has passed its effective reuse period), should be passed to IM&T securely for disposal.

IM&T will be responsible for removing and destroying hard disk drives.

Certificates should be obtained if specialist services are used for media destruction.

If IM&T staff destroy media in line with this policy, a record of the destruction must be kept (see 4.6.6).

4.7.2 Hard Disk Destruction

The recommended specification for data destruction is the SEAP 8500 Type II standard used for classified government material. Equipment that complies with this standard assures complete data destruction.

4.7.3 CD-ROM and DVD Destruction

Non-sensitive data held on CD & DVD may be broken into small pieces or should be cross-cut shredded and disposed of as normal waste.

Sensitive data held on CD & DVD must be either destroyed by an approved contractor or cross-cut shredded and disposed of as secure waste.

4.7.4 Solid-State Devices

Solid-state devices normally consist of Flash USB drives or memory storage cards for PDAs and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction by brute force or incineration is required of the device is required to ensure that any recovery of data is impossible

If the device has previously contained sensitive or person identifiable data, destruction should be carried out by specialist services and certificates obtained.

4.7.5 Magnetic Tape Backup

The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Physical destruction should take place after the tape is appropriately degaussed.

IMPLEMENTATION PLAN	
Intended Audience	For all staff
Dissemination	Available to all staff on the Pulse
Communications	Revised Procedure to be announced in the RIB and a link provided to the document
Training	IG awareness to all staff. Use of encryption – methods and suitability of use. Awareness to staff of what defines sensitive or personally identifiable data.
Monitoring	Scheduled audits of information flow – internally and externally

Glossary

- Bulk data

  20 or more records

- External 3rd party

  Suppliers providing a service to the Trust

- Internal 3rd party

  Contract staff working alongside permanent staff within the Trust

- Removable media

  Storage media which can be removed from its reader device, conferring portability on the data it carries.

- Security Zones

  A security zone is an area or department that processes similar types of information, be it non-sensitive or sensitive.

  Any media passing from any different zones must be afforded appropriate protection to maintain the security of the information stored.

  For example, media used by a department that does not process sensitive data must not be replaced with media used by a department that does without purging of the existing data.

  This model also must be followed if non-sensitive handling media is to be used in an area where sensitive data will be stored on the media.

Appendix 1

Effective Storage Times of Removable Media

Removable Media	Storage Time
CD/DVD	5 years
USB Key	3 years

Note that these time spans are dependant on frequency of use as well as wear and tear.

These media are not reliable as permanent backup media, and should only be used for short-term storage.