London Ambulance Service NHS
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 April 2019.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
12/05/16	3.1	IG Manager	Document Profile and Control update
01/12/15	2.3	IG Manager	Minor amendments and comments
25/11/15	2.2	IS Manager	Minor amendments
07/11/12	2.1	IG Manager	Document Profile and Control update
04/09/12	1.4	IS Manager	Further revisions
13/08/12	1.3	IG Manager	Amendments and comments
17/07/12	1.2	IS Manager	Revision
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
SMT	13/04/16	3.0
ADG	31/10/12	2.0
Information Governance Group	03/02/09	1.0
Ratified by:		
RCAG	16/02/09	1.0

Published on:	Date	By	Dept
The Pulse (v3.1)	17/05/16	Governance Administrator	G&A
The Pulse	08/11/12	Governance Co-ordinator	GCT
The Pulse	09/03/09	Records Manager	GDU
LAS Website (v3.1)	17/05/16	Governance Administrator	G&A
LAS Website	08/11/12	Governance Co-ordinator	GCT
LAS Website	11/03/10	Records Manager	GDU
Announced on:	**Date**	**By**	**Dept**
The RIB	17/05/16	IG Manager	G&C
The RIB	13/11/12	IG Manager	GCT

EqIA completed on:	By
19/01/11	IS and IG Managers
Staffside reviewed on:	**By**

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 and managed throughout its lifecycle. 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. Scope

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

3. Objective

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

4. Responsibilities

Chief Information Officer

- 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.

Caldicott Guardian

- The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and this procedure supports the Caldicott function.

Directors

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

Information Security Manager

- Identifies and implements any configuration requirements necessary 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.

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.
- 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 for work purposes 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) 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 IG contractual terms or an information sharing agreement which would be drafted in line with the broad principles of the Information Security Policy.
- Are responsible for ensuring the security of any data supplied by the Trust.

5. Definitions

Encryption algorithms	Encryption Algorithms are used to mathematically scramble information in a manner very difficult to attack. Current LAS requirements are a minimum of 256bit strength algorithms, such as AES256 may be used.
Hashing function/Checksum	A mathematical algorithm that creates a unique digital value representing the file. If the document is changed it will produce a different value. SHA-256 algorithms are recommended for LAS.
Anonymisation/Redaction of data	Personal data that has been stripped of identifying information meaning it can not be attributed to an individual. Frequently used in research or system testing it is much less sensitive than person identifiable data
Data at rest	Refers to data stored on static media such as a hard disk or CD. Data at rest should be protected by encryption mechanisms so unauthorised access to the media does not result in data loss
Data in transit	Refers to data being transported, usually over a network. Data in transit should be protected in case of interception.

6. Principles of Electronic Information Handling

a. Restricting access to sensitive data

i. It is essential to identify and separate sensitive data from information that is readily available to all internal network users. The separation of this data from normal business directories should be based on the impact of any data exposure. This can be achieved through authentication and authorisation rules set up by IM&T. This is commonly referred to as Controlled Access Based on the Need to Know.

ii. Typically a system handling sensitive data will require a granular access system, where different users have different permissions to perform actions. This is commonly referred to as Role Based Access Control.

iii. Staff and project members working with sensitive data must assess the access and roles of their service and conduct a risk assessment exercise, which will include a privacy impact assessment. Please contact the Information Security Manager for guidance in this.

b. Protecting data in transit

i. Sensitive data must be protected while being transferred; this means the data must be subject to some form of strong encryption. This typically takes one of two forms:

1. Data being transmitted over networks (Internet, email, file transfer, etc), this is covered in section 7.0
2. Data being transferred on removable media (USB sticks, external hard drives, CD, DVD etc), this is covered in section 8.0.
3. Built in password protection features within applications, such as MS Word, MS Excel, etc, do not provide sufficient protection to protect sensitive data and therefore must not be used as the sole method of protection.

c. Protecting data integrity

i. Data integrity may be a requirement, particularly when exchanging batches of information. Consideration should be given to verifying data exchanges to mitigate the consequence of data arriving out of sequence or batches going missing.

d. Protecting data at rest

i. The storage area where databases and directories are stored will need to be considered. Typically hard disks containing sensitive data will require encryption as part of a hardened operating system build.

ii. Additional consideration must be given to how data records are backed up and stored. It is essential that backup data is protected with at least the same level of security as the production data e.g. backups should not be in clear text if the production data is encrypted.

e. Anonymisation/redaction of personal information

Data which cannot identify an individual does not need to be considered as sensitive. *Anonymised, or redacted* data has been stripped of identifying information. *Pseudonymised* data has had identifying items removed, but may be "tagged" with a unique identifier which may enable tracing back to an individual patient. This trace will not be possible by the user, but will be actionable by the originator. Where the user is unable to identify patients, it can be considered as anonymous.

Wherever possible:

- Use anonymous/redacted data
- Only use pseudonymised data where anonymous data will not satisfy requirements
- Only use patient identifiers when neither of the above categories are acceptable.

f. End of life processes

i. A formal process must be in place to ensure media which has carried sensitive data is decommissioned and the data "scrubbed" or the media destroyed. IM&T has arrangements in place to accommodate this including certificates for successfully decommissioned media.

g. Risk Assessment

i. All LAS processes that handle sensitive data are mandated to have a risk assessment exercise conducted against them. The responsible Information Asset Owner should seek advice from the Information Security Manager on how to achieve this.

7. Data Transmission/Transfer over Networks

a. Secure Email Options

The London Ambulance email domain (lond-amb.nhs.uk) is not normally suitable for sending sensitive information; this applies to mail sent to internal users and external bound email. One of the following processes should be used for transferring sensitive data:

i. NHSmail

NHSmail is a centralised, secure email platform for the whole NHS. All mail sent through this system is encrypted and screened for viruses and other malware. LAS staff wishing to transfer person identifiable or sensitive information data, both internally or to other NHS Trusts and third parties should do so with a NHS Mail account. NHS Mail accounts can be requested through the IM&T Service Desk and can be configured for groups and individuals.

ii. Egress Switch

The Trust has recently deployed a solution known as Egress Switch which can be used to transfer confidential or sensitive data to third parties ; Egress employs encryption technologies to secure email communications.

iii. LAS Outlook plug-in

For the LAS supplied Outlook or Outlook Web Access (lond-amb.nhs.uk) to be used to transfer sensitive or person identifiable information, an appropriate encryption utility must be must be purchased and installed. In the first instance, contact the Information Security Manager for advice.

iv. Process for sending encrypted files by email (either than NHSmail or Egress)

If sensitive data is sent by email, it should be encrypted and the decryption key provided by telephone or other method than email. 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 the recipients. Ideally, upon receipt, the recipient must notify the sender, who will then transfer the key.

b. Secure File Transfer Options

Both LAS email and NHSmail accounts restrict the size of file attachments to around 9Mb, which can be restrictive for sharing large files. One of the following processes should be used for bulk transfers of sensitive data:

i. NHS Secure File Transfer

As well as the NHSmail facility, Health & Social Care Information Centre (HSCIC)run a secure file transfer facility specifically for the purpose of transferring sensitive files with other NHS bodies.

https://nww.sft.nhs.uk/sft/upload1

ii. LAS Secure File Transfer Capabilities

LAS share data with several external entities and are looking to standardise this through the use of a Secure File Transfer Protocol Server. If you require regular sharing of secure data contact the IM&T Information Security Manager for details.

c. Integrity of transmitted data

Where the authenticity of data may be questioned, a hashing function/checksum or digital signatures may be used to confirm integrity of stored or transmitted data records and, where appropriate, the identity of the party who originated the data. Procedures should be in place for the verification of signatures and for recording verification timings.

d. 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. See section 8 for detailed instructions on data removal and media sanitation.

8. Data Transfer on mobile media (CD/DVD/USB sticks etc)

a. All use of mobile storage devices must comply with the following requirements:

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

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

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

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

v. When the information stored on removable media is no longer required for the business it must be returned to IM&T for reuse or destruction using a method that makes recovery of the data impossible. In all cases, IM&T will record the action to remove data or destroy data in an auditable log file.

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

vii. 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 take responsibility for security of their data whenever it is taken off site.

viii. 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).

ix. Loss or misuse of removable media must be immediately reported via the IM&T Service Desk to the Information Security Manager and in accordance with the LAS Incident Reporting Procedure. Loss of any removable media containing personal identifiable information must be reported to the Information Governance Manager.

b. Removable media must comply with the following Data Encryption standard

i. All removable media will be encrypted to the following standards:

Only approved encryption algorithms should be used to encrypt and protect relevant LAS data.

The use of freeware, shareware or proprietary encryption that does not benefit from independent security evaluation or that fails to comply with these standards is not permitted and must be avoided.

ii. 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.

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

c. Electronic storage media in transit - 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. Data may be transferred by post/courier as laid out in the following sections[1]:

[1] Note that judgement may be made to work outside the following categories where circumstances dictate, please refer to the Information Security Manager for advice.

i. .Standard Post is suitable for the transfer of:

An encrypted mobile storage device containing up to 10 sensitive records, including personal confidential data. Note the encryption key must not be included in this package and should be exchanged *after* the package has been confirmed as arrived at its destination;

Information that poses minimal risk if the data is lost;

Personal confidential data that has been sufficiently redacted to the point that no single individual can be identified.

ii. Registered/Recorded (Special Delivery) Post is suitable for the transfer of:

An encrypted mobile storage device containing up to 100 sensitive records, including personal confidential data. Note the encryption key must not be included in this package and should be exchanged *after* the package has been confirmed as arrived at its destination;

Personal confidential data about one person that is deemed sensitive and could result in significant harm or distress to an individual;

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.

iii. Secure Courier is suitable for the transfer of:

An encrypted mobile storage device containing up to 1000 sensitive records, including person identifiable data. Note the encryption key must not be included in this package and should be exchanged *after* the package has been confirmed as arrived at its destination;

Encrypted, highly sensitive, non-personal data, where unauthorised disclosure could cause the Trust significant damage to the Trust's reputation and/or prolonged media interest;

Encrypted, highly sensitive data that could cause endangerment to a large number of individuals and/or wide scale damage to the Trust or HM Government interests.

d. Procedures for use of secure couriers

- Authority to dispatch information must be obtained in writing/email from a relevant Director. Subsequent authority to use courier service is obtained from Line Managers. In all cases a record of each authorisation must be maintained in the Department.
- Packaging must be checked to ensure it is sufficient to protect the contents from physical damage.
- Data encryption is tested within the Department by a separate individual to the one who encrypted the data.
- The identification of courier is checked before handover of media. The sender signs the courier's signature sheet.
- A telephone call to notify despatch is made from the despatching organisation to a named individual in the receiving organisation.
- Nominated staff at the destination receives the media and signs the courier's signature sheet. The recipient then notifies sender who supplies the encryption pass-phrase via telephone.

- Immediately after data has been transferred and verified the disks or other media are to be destroyed by the receiving party by cross cut shredding or secure disposal.

e. Media received from external parties

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 handle any sensitive/protectively marked data, please contact the Information Security Department for advice.

f. 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. See section 8 for detailed instructions on data removal and media sanitation.

9. Data Removal, Sanitation and Destruction

All LAS sensitive data must be disposed in a secure manner, the responsibility to carry this out is divided between IM&T and the user of the equipment. The following responsibilities are mandatory:

IM&T are responsible for hard disks (internal and external), portable devices, such as mobile phones and smartphones, and USD memory stick devices. To arrange these tasks the IM&T Service Desk should be informed of the requirement so they can alert the appropriate IM&T function to carry out the task. Sections 9.11 to 9.1.8 refer to IM&T tasks.

Functions outside of IM&T are only authorised to carry out destruction of CDs and DVDs. Section 9.1.9 refers to Local capabilities and responsibilities.

i. Data 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.

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.

ii. Purging Data from reusable media

Purging is required to ensure that when media is removed from its current security context the previous 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 outsourced to a certified third-party supplier.

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.

iii. Media Destruction

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.

IM&T staff or specialist third parties should record each item destroyed (along with the verification results) and maintain this record in a suitable location.

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.

iv. Media Log

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.

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.

v. 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.

vi. 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.

vii. 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.

viii. 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, the IM&T Security Team can purge the data or organise destruction by specialist services.

ix. Local Disposal of Media

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 local cross cut shredder and disposal of any shredded media as secure waste. This must occur in line with the Waste Management Policy.

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.

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

IMPLEMENTATION PLAN				
Intended Audience	All staff			
Dissemination	The Pulse			
Communications	RIB announcement (with other policies)			
Training	Non required, should be BAU			
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**
Destruction records are maintained by IM&T	Annual Audit, results to be included in security capability report to IGG	IM&T Security and Desktop Services	IGG	More incorporation into asset management needed once ITSM is capable

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, not for the archiving of records.

Appendix 2

Tips for importing data from external networks

Information imported from outside the LAS e.g. from the Internet, Industry or partners may contain malware (viruses). In some cases this may be added by a third party without the originator being aware. It is important therefore that where the risk of malware is high, such as when visiting potentially suspect websites, material is handled appropriately. There are a number of ways to reduce the risk of successful exploitation by malware:

- Limit the number of users who have access to content from elsewhere and wherever possible maintain an audit trail of where it has been distributed. This will help clean up process in the event of malware being discovered.
- Ensure that machines that will handle the data are included in the anti-virus update list. These machines must not have the on-access anti-virus feature disabled. Remember that anti-virus can only protect against malware it knows about, new types of malware may not be detected by an anti-virus product..
- Consider using stand-alone, fully patched, dedicated terminals running up to date software for accessing and processing content. Consider using a read-only virtual machine that can be restored to an earlier, known, clean state. It is not recommended but if the terminal needs to be connected to a network, ensure that it is properly segregated from that network and is proactively monitored for signs of unusual activity.
- Lockdown the workstation and turn off features and services that are not required to process the data, e.g. JavaScript or Flash.
- Potentially malicious content should only be processed on the stand-alone terminals. Transfer only the minimum amount of data necessary to your systems using approved import / export procedures and limit import to simple data types only e.g. by extracting text or images from documents. Ensure that any recipients are aware of the source of the material.
- Be aware that when importing information there may be an increased risk by virtue of the fact that your NHS IP address can be identified as such.