London Ambulance Service NHS
NHS Trust

Information Governance Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document:

The purpose of this document is to provide London Ambulance Service NHS Trust staff with a simple framework through which the elements of Information Governance will be met.

Sponsor Department: Information Management &Technology/Governance & Compliance

Author/Reviewer: Information Security Manager and Information Governance Manager. To be reviewed by February 2015.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
16/02/2012	1.3	IS & IG Managers	Further amendments
14/02/2012	1.2	Information Governance Manager	Review and update
27/12/2011	1.1	Information Security Manager	Rewrite and reformat
08/07/2010	0.4	Information Security Manager	Updated comments, minor amendment
07/07/2010	0.3	Head of Records Management	Additional formatting, minor comments
06/07/2010	0.2	Senior Information Risk Owner	Initial review-minor comments
13/06/2010	0.1	Information Security Manager	Document creation

*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
ADG	24/02/12	2.0
SMG	14/07/10	1.0

Published on:	Date	By	Dept
The Pulse	27/07/10 (v.1)	Records Manager	GDU

LAS Website	27/07/10 (v.1)	Records Manager	GDU
Announced on:	Date	By	Dept
The RIB	03/08/10 (v.1)	Records Manager	GDU

EqIA completed on	By
05/06/10	IS Manager; Head of RM; Head of MI
Staffside reviewed on	By

Links to Related documents or references providing additional information	
Ref. No.	Title
TP/012	Data Protection and Confidentiality Policy
TP/022	Freedom of Information Policy
TP/029	Trust Policy Records Management
TP/046	Registration Authority Policy and Procedure
TP/048	Information Security Policy
TP/061	Safe Haven Policy and Procedure

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

This is a high level document that sets out the London Ambulance NHS Trust (otherwise referred to as “LAS”, “The Trust” or “The Organisation” in this document) policy for the handling of information, and in particular, guidance and tools associated with the use of confidential and person identifiable information.

Information is a vital asset and resource, both in terms of the clinical management of individual patients and the effective management of services and its support. Information plays a key role in clinical governance, service planning and performance management.

It is of paramount importance that information is efficiently managed; that appropriate accountability, standards, policies and procedures provide a robust governance framework for information management. Additionally, Information Governance includes the requirement to measure compliance and produce year on year improvement plans.

The organisation aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage with others.

2 Scope

This policy applies to all LAS staff and contractors who undertake any activity for the Trust. It covers all aspects of information use within the Organisation including but not limited to:-

- Patient/Client Service user information;
- Personnel information;
- Corporate Information.

The Policy covers all aspects of handling information including, but not limited

to:-

- Structured record systems-both paper and electronic;
- Transmission of information- including by fax, email, post and telephone.

This policy covers all information systems purchased, designed, developed and managed on behalf of the LAS and any individual directly employed or otherwise by the Trust.

3 Objectives

This Policy aims to provide:

- LAS staff with a framework for the management of the Trust’s information assets;
- Assurance that relevant legal requirements and support for the provision of high quality care by promoting the effective and appropriate use of information, is in place;
- Staff with the tools to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- Support arrangements and appropriate tools to support staff to discharge their Information Governance responsibilities to consistently high standards.

4 Responsibilities

Trust Board

The Trust Board has overall responsibility for Information Governance and will regularly receive reports regarding Information Governance performance from the Risk, Compliance and Assurance Group (RCAG). These reports will detail progress in implementing annual improvement plans for achieving compliance with the Information Governance Toolkit (IGT).

The Chief Executive has overall responsibility for all aspects of the management of this policy.

Senior Information Risk Owner (SIRO)

The Director of Information Management and Technology is the Board Lead for Information Governance with the responsibility for representing Information Governance interests at the Board and Management Committees throughout the Trust. He /she is the nominated Senior Information Risk Owner (SIRO)

Director of Corporate Services

The Director of Corporate Services has strategic responsibility for Information Governance throughout the Trust

Information Governance Group (IGG)

This group's mandate covers all elements of Information Governance and consequently deals with all issues of compliance and acts as a point of reference for queries and problems raised by staff, patients and others. This group will also be responsible for completion of the annual assessment against the Information Governance Toolkit, developing annual improvement plans, monitoring progress on implementing those plans and reporting to the Trust Board. The activity of the IGG will be reported regularly to the Risk, Compliance and Assurance Group (RCAG). .

Caldicott Guardian

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

Assistant Director Corporate Services

The Assistant Director Corporate Services has responsibility for the Governance and Compliance team which includes Information Governance.

Information Governance Manager

The Information Governance Manager takes the lead on Freedom of Information, Data Protection, Access to Health Records, Environmental Information Regulations, Records Management and Data Quality.

Responsible for the management and yearly submission of the Information Governance Toolkit assurance assessments including monitoring compliance levels, and monitoring the development of legislation and guidance as it affects the use of information within the Trust.

Information Security Manager

The Information Security Manager is responsible for the management of information security in the LAS.

Head of Management Information

The Head of Management Information is responsible for the management of health records by staff in MI and Operational Information and Archives.

Information Asset Owners

The Trust has nominated senior managers to oversee the issues of compliance with Information Governance requirements. They are nominated as Information Asset Owners with responsibility for particular Information assets.

IAOs are responsible for implementing procedures to minimise risk e.g. risk of fraud / theft / disruption of critical systems and provide assurance to the SIRO that information is being correctly managed in their areas.

Information Asset Administrators

IAOs, where appointed by IAOs, are staff with day to day responsibility for managing risks to information assets and are most likely to be responsible for one or more individual databases or systems.

Line Managers

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. It is their responsibility to ensure that individuals are made aware of their responsibilities through documentation and awareness sessions, including ensuring new and existing staff complete Information Governance Training as required.

Human Resources

Human Resources must ensure that the contracts of permanent and temporary staff contain clauses that clearly identify responsibilities for confidentiality, data protection and information security and must take reasonable steps to vet all staff before permitting them to access systems and information.

All staff and third parties

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

Additionally each individual, carrying out work on behalf of the Trust, has a personal responsibility to comply not only with the law but also with provisions laid down in their contracts of employment supported by organisational guidelines and documented best practice.

5 Key Governance Elements

There will be proactive management of information within the LAS, both for patient care and service management as determined by law, statute and best practice.

There will be proactive management of information between the Trust and other NHS and partner organisations to support patient care as determined by law, statute and best practice.

There is a commitment to openness, through the Trust's Freedom of Information Publication Scheme, which involves making non-sensitive information widely available in line with responsibilities under the Freedom of Information Act 2000.

Effective arrangements are in place to ensure the confidentiality, security and quality of personal and other sensitive information and to ensure Information within the Trust is of the highest quality in terms of accuracy, timeliness and relevance.

The Trust will ensure it;

- Holds information securely and confidentially;
- Obtains information fairly and efficiently;
- Records information accurately and reliably;

- Uses information effectively and ethically; and,
- Shares information appropriately and lawfully.

6 Statement of Compliance

The Information Governance Statement of Compliance is the process by which organisations enter into an agreement with NHS CFH for access to the NHS National Network (N3). The process includes elements that set out terms and conditions for use of NHS CFH systems and services including the N3, in order to preserve the integrity of those systems and services. An annual assessment will take place prior to compliance sign off by the SIRO.

7 Third Party Contractors

All NHS Trusts are required to ensure confidential information is protected from inappropriate disclosure. Furthermore, under principle one of the Data Protection Act 1998 personal information must be processed (disclosed) lawfully.

In order for the Trust to comply with these duties the Trust will ensure the third parties with whom they contract are subject to, and comply with, patient confidentiality, information security and data protection requirements.

Where the Trust has third parties gaining access to their assets, or the location of their assets, for example cleaners, security guards, auditors, management consultants etc., it is essential that contractors ensure their staff are made aware of the Information Governance requirements by reading the Trust Confidentiality Code of Conduct.

The growth of shared and provider services in the NHS has led to the Trust outsourcing some information processing responsibilities. The Trust will therefore ensure that information governance requirements and procedures in outsourcing contracts meet its business needs.

The Trust will take all reasonable steps to ensure that the contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential.

Third party contractors and their sub-contractors and/or partner organisation are required to formally document their intention to indemnify the Trust against breach of the information governance requirements in the performance of their contract.

Breach of information governance requirements by the third party contractor or their sub-contractor and/or partner organisation may result in immediate termination of the contract.

In addition to the contractual performance requirements above, the Trust will also ensure that any third party contractor is aware of the possible impact of the Freedom of Information Act 2000 on the documentation connected with that contract. For further guidance refer to the Freedom of Information Policy TP/022.

8 Notification of Breach

Managers are responsible for recording all actual and near miss incidents involving any aspect of Information Governance. They will report Information incidents on the LA52 Incident Report Form, sending details through to the Governance and Compliance team who will categorise by severity and record action taken as per the requirements of the Serious Incident Policy (TP006).

Third party contractors, partners or provider organisations are required to notify LAS immediately if a breach, or suspected breach, occurs that may involve LAS information.

In the event of a major breach or significant loss of data the Trust will declare a Serious Incident (SI) as defined in the Serious Incident Policy TP006.

9 Disciplinary Process

Any member of staff in breach of information governance contained within this policy, or other policies supporting it, may be subject to the Trust's disciplinary procedure.

10 Information Governance Framework

The LAS Information Governance framework provides a consistent way for employees to deal with the many different information-handling requirements, which include;

• Information Governance Management

• Confidentiality and Data Protection (including the Data Protection Act 1998)

• Information Security (including ISO/IEC17799:2005)

• Clinical Records Management

• Corporate Records Management (including Freedom of Information Act 2000)

The framework allows the LAS and individuals to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

An assessment of compliance with requirements within the Information Governance Toolkit will be undertaken each year. The results of the return will be monitored along with any action/development plan by the Information Governance Group.

The Information Governance Group via the Information Governance lead will report on the progress of the Trust against the Action Plan and Toolkit to the Board. The annual assessment will be submitted to the Board for ratification. The requirements are grouped into the following initiatives:

- Information Governance Management
- Confidentiality and Data Protection
- Information Security Assurance
- Clinical Information Assurance
- Corporate Information Assurance

10.1 Confidentiality and Data Protection

The Trust will ensure that all staff members are aware of their individual responsibilities regarding data protection and confidentiality issues and also aware of how the work area links with the broader Information Governance agenda.

The Caldicott Guardian plays a key role ensuring that NHS and partner organisations satisfy the highest practical standards for handling patient information and effectively communicating with patients.

Acting as the conscience of the Trust, the Caldicott Guardian also actively supports work to facilitate and enable sharing, advising on options for lawful and ethical processing of information required.

The Trust is responsible for security and confidentiality of personal information it processes. Processing may include the transfer of information to countries outside the European Economic Area (EEA).

Where this is the case a transfer will not be made unless that country has an adequate level of protection for the information and or the rights of individuals.

The Trust will regularly review the flows of patient and personal information from the Trust to understand whether any such information flows outside of the EEA

Key responsibilities within Confidentiality and Data Protection are to:

- implement the Data Protection and Safe Haven Policies
- ensure the Trust complies with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedures and training.
- Complete the Confidentiality and Data Protection Assurance component of the annual toolkit assessment
- Provide routine reports to the Information Governance Group on Confidentiality and Data Protection issues
- To ensure appropriate and effective communications with patients

For further information refer to the Data Protection Policy TP/012

10.2 Information Security

The Information Security Policy (TP048) is a companion document to this Policy and plays a key role in ensuring that all processing of personal and sensitive information satisfy the highest practical standards for ensuring information security.

The IM&T Information Security Manager provides routine reports to the Information Governance Group on Information Security issues.

10.3 Records Management

The Trust will ensure that all staff members are aware of their individual responsibility regarding clinical and corporate record issues and also aware of how the work area links with the broader Information Governance agenda.

The Information Governance Manager plays a key role ensuring that all creation, filing, indexing, storage, disposal and archiving of clinical and corporate records satisfy the highest practical standards for records management.

Key responsibilities within Records Management are:

- To ensure the records work programme is successfully co-ordinated and implemented
- To implement the Records Management and Information Lifecycle Policy
- To ensure the Trust complies with the principles contained in the Records Management: NHS Code of Practice and that staff are made aware of their individual responsibilities through policy, procedures and training
- Complete the Clinical Information and Corporate Information Assurance components of the annual toolkit assessment
- Provide routine reports to the Information Governance Group on records management issues

10.4 Registration Authority Management

The Trust will ensure that all relevant staff members are aware of their individual responsibility regarding the registration authority and system access control issues and also aware of how the work area links with the broader Information Governance agenda.

The Registration Authority plays a key role ensuring that all new user registrations of `smartcards` are completed in accordance with the Registration Authority Procedure to satisfy the highest practical standards for Registration Authority management, together with the principles detailed by the NHS which govern how patient information is accessed and shared.

Key responsibilities within Registration Authority Management are:

- To ensure the registration authority work programme is successfully co-ordinated and implemented
- To implement the Registration Authority Policy, procedures and terms and conditions of use
- To ensure the Trust complies with the principles contained in the NHS guidance and that staff are made aware of their individual responsibilities through policy, procedures and training
- Complete the Registration Authority Management component of the annual toolkit assessment
- Provide routine reports to the Information Governance Implementation Group on Registration Authority issues

10.5 Legal Compliance

The Trust regards all personal identifiable information as confidential except where national policy on accountability and openness requires otherwise.

The Trust will undertake to commission annual assessments and audits of its compliance with legal requirements.

The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other NHS organisation and partner agencies, taking account of relevant current legislation.

11 Training

To maintain its information handling standards throughout the organisation, the LAS will ensure that all staff are provided with clear guidelines on their own obligations for confidentiality, data protection and information security.

11.1 Staff Awareness Training

The Trust must comply with all aspects of the law that concern the processing of personal data. This includes legislation (Acts of Parliament), regulations, common law duties and professional codes of practice.

It is vitally important that new staff are made aware of the relevant requirements and in particular given clear guidelines about their own individual responsibilities for maintenance of Information Governance, and that existing staff complete refresher training periodically. Particular emphasis will be placed on how the requirements affect their day to day practices

As a minimum the induction training includes:

- The duty of confidentiality
- Sanctions for breach of the duty of confidentiality
- Keeping personal information private, e.g. avoiding gossip and inappropriate venues for discussion of patient care
- The use of security measures to ensure information is not inappropriately disclosed e.g. closed doors, locked cupboards, password management etc.

- The frameworks in place to allow appropriate disclosure
- Dealing with subject access requests
- Freedom of Information Act responsibilities
- The importance of accurate information capture
- Pointers to where the Trust policies, procedures and further information are located.

12 Audit, Monitoring and Review

The Information Governance Group will be responsible for leading on the implementation of this policy and other Information Governance related policies and procedures. It will ensure that clear formal guidelines have been provided to staff on all aspects of Information Governance.

The review or creation of other Information Governance related policies and procedures will include mechanisms for monitoring compliance with this policy or other procedure standards.

This policy will be continually monitored and will be subject to regular review, which will take place annually from the date of issue. An earlier review may be warranted if one or more of the following occurs:

- As a result of regulatory / statutory changes or developments
- As a result of NHS policy changes or developments
- For any other relevant or compelling reason

IMPLEMENTATION PLAN	
Intended Audience	All Staff
Dissemination	Pulse and LAS website
Communications	Announced in the RIB
Training	New staff will be provided with Information Governance training at their Corporate Induction and as part of their local induction. All staff are required to complete the online training modules – 'Introduction to Information Governance' or 'Information Governance: the Beginners Guide'. On an annual basis all staff must now complete the online 'Information Governance Refresher Module'. The three year core training refresher course for support staff also includes Information Governance.
Monitoring	Adherence to all aspects of the policy will be monitored through Independent Audits, spot checks, and employee feedback. Monitoring will be the responsibility of the Information Governance Group and will take place annually and also as part of the IGToolkit work improvement plan.

Appendix 1

Legislation and Guidelines

It is LAS policy to fully comply with all applicable legislation and regulations, in particular, the following laws that are particularly applicable to information security.

- Official Secrets Act 1989
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- The Human Rights Act 1998
- The Equality Act 2010
- Privacy and Electronic Communications Regulations 2003 and 2004
- The Regulation of Investigatory Powers Act 2000
- The Interception of Communications Act 1985
- Electronic Communications Act 2000
- The Design Copyright and Patents Act 1988
- Police and Criminal Evidence Act 1984
- Crime and Disorder Act 1998
- Civil Contingencies Act 2004
- The Health and Safety at Work Act 1974
- The Lawful Business Practice Regulations 2000
- The Public Records Act 1958
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- The Crime and Disorder Act 1998
- The Caldicott report
- The Information Governance Toolkit
- Re-use of Public Sector Information Regulations 2005
- DoH Confidentiality – NHS Code of Practice
- The NHS Care Record Guarantee

Appendix 2

Information Governance Toolkit Compliance Statement

The LAS are required to provide an appropriate level of information governance based upon the requirements of the Information Governance Toolkit (IGT). This Policy supports the following requirements of the Information Governance Toolkit v9:

Requirement 101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
Requirement 105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans