London Ambulance Service NHS Trust

Confidentiality Audit Procedure

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To establish an approach to monitor access to confidential information throughout the Trust.

.

Sponsor Department: Governance and Compliance

Author/Reviewer: Information Governance Manager. To be reviewed by May 2014

Document Status: Draft

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
18/03/11	0.2	Head RM	Revised draft
09/03/11	0.1	Head RM	New procedure first 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**
IGG	27/05/11	1.0
Agreed by Trust Board (If appropriate):		

Published on:	**Date**	**By**	**Dept**
The Pulse			G&C
LAS Website			
Announced on:	**Date**	**By**	**Dept**
The RIB			G&C

EqIA completed on	**By**
28/03/11	C D-B; SM; BO.
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
TP/006	Serious Incident Policy	
HS/011	Incident Reporting Procedure	
TP/029	Records Management & Information Lifecycle Policy	

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

With advances in the electronic management of information within the NHS the requirement to monitor access to confidential information has become increasingly important. Furthermore, with the increased use of electronic communications, the movement of confidential information via these methods poses an increasing threat of information falling into the hands of individuals who do not have a legitimate right of access to it. Good practice requires that all organisations put in place control mechanisms to manage and safeguard confidentiality, particularly patient and other personal information.

It is recognised that the majority of staff do not willingly abuse the information to which they have access, but the London Ambulance Service NHS Trust has a responsibility to ensure that confidential information is protected. Access needs to be carefully monitored and controlled as failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purpose may result in a breach of that confidentiality, therefore contravening the requirements of Caldicott, the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

This procedure will provide an assurance mechanism by which the effectiveness of controls implemented within the Trust are audited, areas for improvement and concern highlighted, and recommendations for improved control and management of confidentiality within the Trust made.

2. Scope

All work areas within the Trust which process (handle) confidential information will be subject to this confidentiality audit procedure. These work areas have been identified in the information flow mapping tool. Confidentiality audits will focus primarily on controls within electronic systems but access to both electronic and manual confidential information will be audited.

3. Objectives

To establish an approach to monitor access to confidential information throughout the Trust.

To provide assurance that the necessary controls are in place to manage access to confidential information

To discover whether confidentiality has been breached, or put at risk, through misuse of systems, or as a result of poorly applied controls.

4. Responsibilities

The **Chief Executive** has overall responsibility for ensuring that Information Governance is managed responsibly within the Trust.

The **Director of Corporate Services** has strategic responsibility for Information Governance including monitoring and auditing access to confidential personal information.

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

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

The **Information Governance Manager** is responsible for ensuring that a confidentiality audit procedure is developed and communicated to all staff with the potential to access confidential information.

The **Information Security Manager** is responsible for information security in the LAS, for implementing security actions arising from confidentiality audits and reporting any concerns highlighted as a result of monitoring access to confidential information through to the IGG.

The **Information Governance Group (IGG)** is chaired by the Director of IM&T who is the Senior Information Risk Owner (SIRO) and will monitor the implementation of this procedure.

The **Information Governance Working Group (IGWG)** is responsible for drawing up the programme of peer review audits in conjunction with the Information Governance Manager and members of the Group will liaise with the IG Manager on audits that take place in their areas..

The **Senior Management Group** and **Heads of departments** are responsible for ensuring that this procedure is implemented in their directorates and individual departments.

Information Asset Owners (IAOs) have a responsibility to provide assurance that information risk is being managed effectively in respect of the information assets that they ‘own’.

Information Asset Administrators (IAAs) have day to day responsibility for managing risks to one or more individual databases or systems.

5. Controls and Monitoring Access to Confidential Information

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary to have appropriate controls in place and ensure monitoring is undertaken on a regular basis. For structured systems monitoring should be carried out by the IAOs or IAAs on a regular basis in line with system procedures/controls. For unstructured information, such as MS Word documents, monitoring should be carried out by records supervisors in order to check that controls are in place in line with Appendix 1 of TP/029 Records Management and Information Lifecycle Policy and irregularities regarding access to confidential information can be identified, reported, and action taken to address the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

6. Reporting and Investigating Confidentiality Incidents

Actual or potential breaches of confidentiality should be reported in line with the Trust's Incident Reporting Procedure in order that action can be taken to prevent further breaches taking place. The Information Security Manager will be responsible for ensuring that the Information Governance Group is informed of any concerns highlighted as a result of monitoring access to confidential information.

Investigation and management of confidentiality incidents will be in line with the Trust's Serious Incident Policy.

Unauthorised access to confidential information by any individual will be considered against the Trust's disciplinary procedures. Any breaches of confidentiality or security made outside the proper course of duty may be considered by a disciplinary panel and treated as a serious disciplinary offence which could lead to dismissal from employment.

7. Auditing Access to Confidential Information

Audits should check:-

- failed attempts to access confidential information;
- repeated attempts to access confidential information;
- access of confidential information by unauthorised persons;
- evidence of shared login sessions/passwords;
- previous confidentiality incidents and actions, including disciplinary, taken;
- Staff awareness of Trust policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;
- Appropriate communications with patients;
- Appropriate recording and/or use of consent forms;
- Appropriate use of smartcards;
- Appropriate allocation of access rights to systems which contain confidential information;

- Appropriate staff access to physical areas;
- Storage of and access to filed hard copy patient notes and information;
- Security of post handling areas;
- Security of confidential fax handling;
- Appropriate use and security of desk and mobile telephones in open areas;
- Extent of using and handling protectively marked documents;
- Confidential information sent or received via e-mail, security applied and e-mail system used ;
- Information removed from the workplace - has authorisation been gained either for long-term or short term removal?
- Security applied to laptops and portable electronic media;
- Evidence of secure waste disposal;
- Use of whiteboards for confidential information;
- Information flows of confidential information;
- Appropriate transfer and sharing arrangements are in place;
- Security and arrangements for recording access applied to manual; files both live and archive, eg storage in locked cabinets/locked rooms.

8. Audit Method

8.1 Audits will be carried out in one of two ways:

a) Through the annual internal audit programme where a department or areas of the Trust have been identified for a confidentiality audit or as part of a records or other Information Governance audit. These audits will be carried out by the Trust's internal auditors in conjunction with Directors, department heads and other appropriate staff.

b) Through peer review by one department on another. Following knowledge obtained through the Records audits and the Information Flow map a listing of appropriate departments/areas in the Trust will be produced by the Information Governance Manager and Information Security Manager. A programme of audits will then be drawn up annually by the Information Governance Manager in conjunction with the Information Governance Working Group (IGWG) which will be presented to the Information Governance Group for approval. Once approved, departments will be alerted to the programme and matched prior to the audit dates being agreed. Each audit will have a reference number to be used on all documentation and should be carried out by the appropriate member of the IGWG, or other member of the reviewing department's staff as agreed with the department head, through a series of interviews with Heads of Department, IAOs, IAAs, Records Supervisors and Staff.

8.2 Frequency

Internal Audits will take place as identified in the annual internal audit programme and peer review audits will be planned so that all identified departments and areas will be audited on a two year rolling programme.

8.3 Peer Review Audits

8.3.1 Pre-Audit Questionnaires

It will assist the audit process for the area to be audited to complete a pre-audit questionnaire (see Appendix 1) which will enable the auditor to gain an understanding of the function of the department and the processes carried out relating to confidential information. This will allow the auditor to ask informed questions when conducting the audit. The pre-audit questionnaire should be annotated with the name of the department or area, a contact name and number and should be returned to the auditor in advance of the scheduled audit date.

8.3.2 Pre-Audit Meeting

Unless the questionnaire provides all the necessary background information required the auditor should arrange a brief pre-audit meeting with the department head, IGWG member, or Records Supervisor with the aim of discussing the process and what documentation will be required. The required documentation, including local procedures which are in place, should be forwarded to the auditor prior to the audit commencing.

8.3.3 Audit Checklist

An Audit Checklist (see Appendix 5) should be used to detail the elements to be checked (as listed in section 8). This will enable the auditor to track progress of the audit.

9. Conducting the Audit

9.1 Audit Checklist

Brief notes should be made on the Audit Checklist as follows:

Column B should be used to record evidence put forward to support the responses to questions asked. Where documents form the evidence provided, the reference number of the document or documents should be included for ease of reference.

Column C should be used to record the auditor's assessment as to how the evidence demonstrates compliance with the requirements of the Data Protection Act, the procedures and the Caldicott Principles.

Column D should be used to record the auditor's grading of the response to each question:

- COM – evidence demonstrates fully compliance
- MAJ – evidence demonstrates major non-compliance
- MIN – evidence demonstrates minor non-compliance

9.2 Staff Awareness

In addition to the above the auditor should consider carrying out staff awareness interviews. The following should be considered:

• Roles and responsibilities;
• Awareness of general confidentiality issues;
• Understanding of Data Protection Principles directly relating to their job;
• Understanding the requirements of policies and procedures relating to confidentiality;
• Training received.

The auditor's questions and the interviewee(s) responses should be recorded on the Interview Record Sheet – See Appendix 2.

10. Reporting

10.1 Non-Compliance

Where non-compliance is observed, this should be recorded as soon as possible, be sufficiently detailed, including all the facts and referring to any relevant evidence. The non-compliance should be recorded on the Non-compliance Observation Sheet – Appendix 3. The detail recorded should include an outline of what was observed, where it was observed, who was involved, the date of the observation and why it was considered non-compliant. Each non-compliance observed should have an associated recommendation which should be discussed and agreed with the head of department and other staff as appropriate. Each recommendation should also include a target date for completion and a named individual who will be responsible for ensuring that the recommendation is implemented. Once the follow-up meeting has taken place the auditor will complete the bottom section of the form, indicating implementation of recommendations and effectiveness of those recommendations. When the auditor is satisfied that the non-compliance has been resolved the auditor will sign the Non-compliance Observation Sheet.

Non-compliance can fall into one of two categories:-

Major Non-compliance: this would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequences.

Minor Non-compliance: these could include one-off occurrences of non-compliance; there are likely to be only minor consequences.

Where a number of minor instances of non-compliance are observed in the same functional area or department, this may indicate a more serious problem within that area. If this is the case, these instances of non-compliance should be combined into a Major non-compliance.

10.2 Report

Once the audit has been completed a formal report should be produced by the auditor (following the template at Appendix 4) detailing the outcome of the audit. It will include a summary of the findings of the audit, together with observations of non-compliance and recommendations which have been made. A meeting should be held with the Head of Department, IAO, IGWG member, or Records Supervisor as appropriate to go through the findings and agree the corrective actions required. Any comments expressing disagreement should be noted on the audit report which, when finalised, should be provided to the area being audited and sent to the Information Governance Manager.

10.3 Quality Assurance

The Information Governance Manager will sample review reports and their supporting documentation in order to verify consistency of approach.

11. Audit Follow-Up

Reports on audit outcomes including progress on recommendations made will be considered by the Information Governance Group who will monitor progress on actions identified.

12. Audit Closure

Once corrective action has been checked and agreed as compliant by the auditor, the audit can be formally closed.

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	Staff who will be required to carry out peer review audits will be given appropriate audit briefings.
Monitoring	The peer review audits and their outcomes will be monitored by the Information Governance Manager as part of the rolling programme and progress will be reported through to the Information Governance Group at each meeting. Results will be monitored by the Risk Compliance and Assurance Group who will receive minutes and reports from the IGG.

Appendix 1

PRE-AUDIT QUESTIONNAIRE

Department:		**Audit Ref.**
Location:		
Contact Name:	**Position:**	**Telephone No:**
Summary of Department Functions:		
Number of Full Time Staff:	**Number of Full Time Staff:**	
Question 1	*Enter Question Here:*	
Response:		
Question 2	*Enter Question Here:*	
Response:		
Question 3	*Enter Question Here:*	
Response:		
Question 4	*Enter Question Here:*	
Response:		

Question 5	*Enter Question Here:*
Response:	

Appendix 2

INTERVIEW RECORD SHEET

Department:	**Audit Date:**	**Audit Ref.** **Page No:**
ATTENDEES		
Name	**Position**	
DETAILS OF INTERVIEW		
Question 1	*Enter Question Here:*	
Response:		
Question 2	*Enter Question Here:*	
Response:		
Question 3	*Enter Question Here:*	
Response:		
Question 4	*Enter Question Here:*	
Response:		
Question 5	*Enter Question Here:*	
Response:		

Appendix 3

NON-COMPLIANCE OBSERVATION SHEET

<table>
<tr><td colspan="2">Department:</td><td>Audit Date:</td><td>Audit Ref:</td></tr>
<tr><td colspan="4">Details of Non-Compliance:</td></tr>
<tr><td colspan="2">Extent of non-compliance
(tick as appropriate)</td><td>Auditor Name:</td><td rowspan="2">Date of observation:</td></tr>
<tr><td>Major</td><td>Minor</td><td>Signature:</td></tr>
<tr><td colspan="4">Recommendations:</td></tr>
<tr><td>Follow-up Date:</td><td colspan="3">Additional Comments:</td></tr>
<tr><td colspan="4">Follow-up:</td></tr>
</table>

Compliance Assessment:	**Auditor Name:**	**Date Re-assessed:**
COM/MIN/MAJ	**Signature:**	

Appendix 4

AUDIT REPORT TEMPLATE

Department:	**Audit Date:**	**Audit Ref.**
		Page No. 1
AUDIT SUMMARY		

Auditor Name:	**Signature:**	**Date Closed:**

AUDIT REPORT TEMPLATE (CONTINUED)

Department:	**Audit Date:**	**Audit Ref.**
		Page No:2

OBSERVATIONS SUMMARY	
Obs Ref	**Details of Observations**

SUMMARY OF AGREED CORRECTIVE ACTIONS			
Non Compliance Ref	**Action By**	**Corrective Action to be Taken**	**Date**

AGREED AUDIT FOLLOW UP		
Auditor Name:	**Signature:**	**Date Closed:**

AUDIT CLOSED		
Auditor Name:	**Signature:**	**Date Closed:**

ADDITIONAL COMMENTS:

Appendix 5

AUDIT CHECKLIST

Department:		**Interviewee:**	**Date:**
Process:		**Auditor:**	**Ref No.**
Question or Check (a)	**Documentary Evidence Examined (B)**	**Findings and Observations (C)**	**Result (D)**