LONDON'S GLOBAL UNIVERSITY

SLMS Confidentiality Audit Procedure

1. **Document Information**	
Document Name	SLMS-IG09a SLMS Confidentiality Audit Procedure
Author	Shane Murphy
Issue Date	02/08/2013
Approved By	Chair of SLMS Information Governance Steering Group (IGSG)
Next review	Three years

2. **Document History**		
Version	**Date**	**Summary of change**
0.1	18/02/2013	First draft for discussion
0.2	07/06/2013	Second draft incorporating comments from Alice Garrett and Bridget Kenyon
0.3	02/07/2013	Third draft incorporating comments from Alice Garrett and Bridget Kenyon
0.4	19/07/2013	Minor changes made following feedback from IDHS Project
1.0	02/08/2013	Approved by Chair of SLMS IGSG

1.0 Introduction

1.1 This procedure establishes appropriate confidentiality audit procedures to monitor access to personal identifiable data throughout the SLMS. This work forms part of the SLMS's Information Governance assurance framework and meets requirements within:

- the NHS Information Governance Toolkit
- the NHS Confidentiality Code of Conduct
- the NHS Care Record Guarantee
- Data Protection Act 1998
- Regulation of Investigatory Powers Act (RIPA) 2000
- Human Rights Act 1998

2.0 Scope of the Audits

2.1 All work areas within the SLMS which handle Personal Identifiable Data (PID) will be subject to the confidentiality audit procedures.

2.2 Access to electronic and manual personal identifiable data will be audited. Audits across all the SLMS's sites will be undertaken and this will capture any inconsistencies in practices.

3.0 Audit Approach

3.1 The Audits will review compliance in the following topic areas, where applicable, to establish evidence:

- Staff awareness of the SLMS policies and guidelines concerning confidentiality
- Appropriate recording of consent
- Appropriate use of dual factor authentication
- Appropriate allocation of access rights to systems
- Appropriate staff access to physical areas
- Secure storage of and appropriate access to filed hard copy person-identifiable notes and information
- Security of post handling areas
- Security of confidential fax handling
- Security of recorded telecommunications and message books
- Appropriate use and security of the telephone in open areas
- Storage of personal identifiable data (PID) in public areas

3.2 The Audit Team will provide the following deliverables:

- A nominated lead responsible officer for implementation[1]
- Detailed audit procedures and auditor specifications
- Trained auditors
- Planned and implemented audit programme
- A spreadsheet or database to record audit findings and outcomes

[1] See Appendix 2

- Audit reports and recommendations for the Information Governance Steering Group (IGSG)
- Support for action plans to address any areas requiring review
- Follow up process for IGSG
- Reports to the Senior Information Risk Owner (SIRO) concerning any identified breaches.

3.3 Audit methods and facilities to be utilised:

- Notified audit visits with structured templates
- Spot checks, with structured templates, to random work areas to confirm PID is used and obtained fairly and lawfully
- Interviews with staff using structured templates
- Regular staff knowledge and understanding surveys[2]
- Results from the IG Toolkit Training Needs Analysis
- Investigation of reports on the IGSG standing agenda for Serious Untoward Incidents (SUIs).

3.4 The IG Lead will arrange an audit programme annually with the Internal Audit Service.

3.5 Audit results will be collected on a standard template and then held for future reporting and analysis.

4.0 Audit Findings

4.1 Results from the audits will be collected in a standard template and then recorded in a spreadsheet or database for future reporting and analysis. The report will be submitted to the Information Governance Steering Group and will highlight any areas requiring further development and make recommendations concerning any corrective actions required. In particular evidence gathered concerning the following should be assessed and reported to the IGSG:

- failed attempts to access confidential information;
- repeated attempts to access confidential information;
- successful access of confidential information by unauthorised persons;
- evidence of shared login sessions/passwords;
- disciplinary actions taken.

5.0 UCL Disciplinary Policy and Procedures

5.1 In the event that there has been an incident of gross misconduct the Audit Lead will invoke the **Disciplinary Procedure**.

5.2 UCL SLMS is committed to the avoidance of formal disciplinary procedures wherever possible by addressing problems as soon as they arise.

[2] Tools to be used include Opinio

Appendix 1 – Definitions and acronyms

IGSG: Information Governance Steering Group. This Group is responsible to the SLMS Senior Executive Group (SEG) for the maintenance of an information governance framework for SLMS. It is responsible for ensuring that Information Governance Toolkit support is available to the SLMS Research Community.

Personal identifiable Data (PID): is defined as any information about a person which would allow that person to be identified. Any inappropriate disclosure of that personal identifiable data would breach their right to privacy, or present a risk of identity theft.

RIPA: Regulation of Investigatory Powers Act 2000. The Act regulates the powers of public bodies to carry out surveillance and investigation, including the interception of communications.

SLMS: School of Life & Medical Sciences

SUI: Serious Untoward Incident, NHS terminology to describe incidents that would have a negative impact to an organisation.

Appendix 2 – Audit Lead Training, Competencies and Responsibilities

The Audit Lead shall undertake Confidentiality Audit Training. Confidentiality audits should be conducted in respect of electronic and hard copy based systems. The purpose of the audits is to discover whether confidentiality has been breached; has it been put at risk due to deliberate misuse and are the controls for information systems sufficiently robust.

The Audit Lead will be expected to be capable of conducting audits and leading teams to:

a. Identify areas of weakness in respect of confidentiality;
b. Reduce the risk of mistakes happening that would result in a breach of confidentiality; and
c. Recommend robust controls to protect confidentiality

The Audit Lead shall provide suitable assurances with formal and verbal reports to IGSG, that controls are working effectively and that appropriate monitoring is part of the overall Information Governance assurance framework.

The Audit Lead shall invoke the Disciplinary Procedure as necessary.