Bolton Clinical Commissioning Group

Confidentiality Audit Procedure

Policy Number	**IG009**
Target Audience	**CCG/GMSS staff**
Approving Committee	**CCG Executive**
Date Approved	**September 2013**
Last Review Date	**July 2016**
Next Review Date	**August 2018**
Policy Author	**IG Manager (GMSS)**
Version Number	**V3**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	M Robinson D Sankey	Progress to CCG Exec Team for approval
1	**September 2013**	**CCG Exec**	**Approved**
2	**November 2013**	**Andrea Hughes**	**Appendix 1 - Template update**
2.1	**July 2016**	**IG Team**	General admin changes. Section 3.5 updated to IM&T Operations Board. No substantial content change required.
3	**August 2016**	**IM&T Operations Board**	**Approved**

Analysis of Effect completed:	By: M Robinson	Date: September 2013

Contents Page

1 Introduction

Bolton CCG and Greater Manchester Shared Services (GMSS) are committed to a programme of effective risk and incident management. Both organisations must ensure that access to confidential information is justified where this is required and monitored locally and that there are procedures for investigating breaches of confidentiality.

This procedure applies to all staff who act for or on behalf of Bolton CCG such as third party contractors and others (e.g. business partners, including other public sector bodies, volunteers, commercial service providers).

This procedure outlines the arrangements adopted by the CCG for the auditing and monitoring or privacy and confidentiality issues in relation to the processing of personal data. It provides an assurance mechanism by which the effectiveness of controls implemented within the organisation are audited, areas for improvement and concern highlighted and recommendations for improved control and management of confidentiality.

2 Aims and Objectives

Confidentiality audits will focus primarily on control within electronic records management systems but also includes paper record systems and confidentiality processes undertaken by departments, for example secure transfers of information processes. The purpose is to discover whether confidentiality has been breached or put at risk through deliberate misuse of systems as a result of weak, non-existent or poorly applied controls.

Assurance that controls are working should be part of the CCG's overall assurance framework. 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 Computer Misuse Act 1990, the Human Rights Act 1998 and the Confidentiality Code of Conduct.

Types of Confidentiality Alerts

- Follow ups of failed log-in reports provided for information systems
- Monitoring of incident reports regarding stolen/lost computers/laptops, disclosure of confidential material
- Reports from confidential audits around Greater Manchester CCG (GMCCG) sites
- Internal audits of reviews of IT security
- Complaints from members of the public / staff
- Informal alerts made by staff
- Reported near misses

3 Accountability and Responsibilities

3.1 Responsibility of the Caldicott Guardian

The Caldicott Guardian has overall responsibility for the monitoring incidents and complaints relating to confidentiality breaches and is responsible for ensuring that access to confidential information is regularly audited within the GMCCG. Recommendations and concerns arising from confidentiality audits are actioned within a reasonable timeframe.

3.2 Responsibility of the Senior Information Risk Owner (SIRO)

The SIRO is responsible for ensuring that the Confidentiality Audit Procedures are in place in order to mitigate information risk within GMCCG.

3.3 Responsibility of the GMSS IG Manager and Lead Information Governance Officers

The Information Governance Manager and Lead Information Governance Officers are responsible for co-ordinating the approach for investigating confidentiality alerts which arise from incidents, complaints, audit reports, informal alerts, failed log-in reports from systems such as People Services systems.

3.4 Responsibility of Managers/Heads of Department/Information Asset Owners

All managers are responsible for ensuring that staff for whom they are responsible for are aware of their responsibilities with regard to confidentiality of information and ensure that staff complete Information Governance training.

Managers are responsible for ensuring that their staff are fully aware of the mechanisms for reporting actual or potential confidentiality breaches within the CCG/GMSS. This is documented in the Information Governance Incident Reporting Procedure (IG007) and can be found on the CCG Intranet.

They are also responsible for complying with confidentiality audits and ensuring that subsequent recommendations are complied with within specified timescales.

Access to electronic and/or manual confidential information must be strictly controlled within each managers/information asset owner's area of responsibility. They will be responsible for ensuring that appropriate authorisation is gained prior to allowing access to confidential records in order that only those individuals with a legitimate right are given access. Such authorisation should be documented and retained for monitoring purposes, this should include information as to who has gained access, their department, the reason access was required, the date access was given etc.

Information should also be recorded relating to failed access attempts where a request for access has been denied or prevented. Regular monitoring should be undertaken in order to highlight potential areas for concern.

3.5 Responsibility of the IM&T Operations Board

The IM&T Operations Board will be responsible for ensuring that the Confidentiality Audit Procedures are implemented throughout the Bolton CCG. The procedure will be approved by this group

3.6 Responsibility of Employees

All staff have a duty to read and work within current policies. They should ensure that confidential information is not accessed without prior authorisation and completion of the appropriate documentation. Confidential information should also not be disclosed to unauthorised recipients.

Any breach or refusal to comply with this policy is a disciplinary offence, which may lead to disciplinary action in accordance with the CCG's Disciplinary Policy, up to and including, in appropriate circumstances, dismissal without notice.

All staff must be aware that Information Governance audits of departments may occur at any time.

4 Monitoring and Auditing Access to Confidential Information

4.1 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 ensure appropriate monitoring is undertaken on a regular access.

Monitoring should be carried out by the Information Asset Owner or delegated to the Information Asset Administrator for a department / system in order that irregularities regarding access to confidential information can be identified. If irregularities are found these should be reported to the Caldicott Guardian / Information Governance Department and action taken by the Information Asset Owner/Information Asset Administrator to rectify the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

Actual or potential breaches of confidentiality should be reported immediately to the Information Governance Department and by logging this as an incident following CCG's incident governance reporting processes in order that the incident can be reviewed and action taken to prevent further breaches. Further information regarding this can be found in the Information Governance Incident Reporting Procedure (IG007).

The Information Governance Team will be responsible for ensuring that the Caldicott Guardian and/or SIRO and the Head of Business Intelligence is informed of any concerns highlighted as a result of monitoring access to confidential information.

Should unauthorised access to confidential information be gained by any individual or if information is disclosed to unauthorised recipients, this will be dealt with in accordance the CCG's Disciplinary Policy.

4.2 Auditing Access to Confidential Information

The Information Governance Department and Caldicott Guardian will ensure that confidentiality audits are conducted on a regular basis. Areas to be audited and should be:

- Audit and observations of any confidentiality or information security breaches
- Security applied to manual files e.g. storage in locked cabinets / locked rooms
- The use of and disposal arrangements for post-it notes, notebooks and other temporary or paper recording material
- Retention and disposal arrangement – confidential waste procedures
- The location of fax machines and answer phones which receive personal, sensitive or confidential information – are they designated safe haven faxes?
- The location of post trays for incoming and outgoing mail – are they located in safe haven areas
- Information removed from the workplace – has authorisation been gained for either long term or short term removal
- The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information
- Checks to ensure staff have read, understood and signed the Confidentiality Code of Conduct/have a employment contract with relevant IG clauses contained within it
- Checks to test staff awareness regarding who to contact regarding Subject Access requests, Freedom of Information requests and how to report incidents
- Checks to ensure security has been applied to portable equipment e.g. laptops and removable media e.g. only encrypted memory sticks must be used with a valid reason why they are being used
- Evidence of shared passwords being used within the department / area being audited
- Observations of good practice regarding assuring the confidentiality of personal confidential information (PCD).

4.3 Method and frequency of audits / monitoring

Confidentiality audit checks will be carried out using a variety of methods. Spot checks and walk round site audits using standard proformas (Appendix 1 and 2) on an annual basis or more frequently where this is required. Questions will be asked to staff and observations made regarding information governance practices.

Areas of non compliance will be reported on the Non-Compliance Observation Sheet (Appendix 2) and fed back to Line Managers/Information Asset Owners for action and follow up. Areas of good practice will also be identified and provide details of compliance with confidentiality requirements.

Where non-compliance/information risks are observed, this will be reported back to the relevant line manager and include recommendations for action and a target date for completion. A named individual (Line Manager, Associate Director) will be responsible for ensuring that the recommendation is implemented. Further checks will be made to ensure the recommendation has been implemented and risks mitigated.

A report will also be produced detailing the outcome and any information risks identified. This will be presented to Bolton CCGs IM&T Operations Board and to the Caldicott Guardian/SIRO/ Head of Business Intelligence when applicable for escalation.

Other methods of audit checks include follow up from complaints, alerts and incidents reported which may involve producing audit reports from an electronic person identifiable record system to check, for example, if a member of staff has inappropriately accessed a record. The frequency regarding this will vary.

Information Asset Owners/Line Managers are expected to undertake regular auditing of their systems to check for any suspicious activity, e.g. failed login attempts or accessing patient or staff details inappropriately. If this is found, it must be reported to bolccg.incidents@nhs.net via the CCGs incident reporting tool available on the intranet http://sg01/safeguard/. The CCG Governance and Risk Department will inform the GMSS Information Governance Leads of any IG incidents so they can be investigated and followed up appropriately.

Upon the request of People Services, the Information Asset Administrators / System Managers are required to produce audit trail reports from their relevant IT systems in order to assist with investigations. This should be transferred confidentially to the lead investigating officer.

4.4 Logging and Reporting of confidentiality alerts/incidents

The CCG's Information Governance Incident Reporting Procedure (IG007) applies and incidents should be reported to bolccg.incidents@nhs.net or via the CCGs incident reporting tool available on the intranet http://sg01/safeguard/. The CCG Governance and Risk Department will inform the GMSS Information Governance Leads of any IG incidents so they can be investigated and followed up appropriately.

Reports relating to IG incidents will be submitted to the Information Governance Management Group and to the Caldicott Guardian/SIRO/Head of Business Intelligence. Exceptional issues will be escalated to the Caldicott Guardian for advice and rectification. Lessons learned will be disseminated through appropriate communication processes as highlighted in the Information Governance Communications Strategy.

5 Training and Awareness

This procedure will be available on the CCG Intranet. Staff are also informed about the reporting of breaches / alerts / incidents via mandatory training. Lessons learned from incidents will be fed back into future training or where appropriate to the staff concerned to encourage further participation and demonstrate the value of reporting to CCG/GMSS staff.

The Caldicott Guardian/SIRO and Head of Business Intelligence are made aware of information governance related incidents/complaints/alerts reported and the associated action plans to mitigate similar incidents occurring in the future.

All staff will continue to be informed about the importance of reporting information governance related incidents via a variety of media such as handouts, leaflets, intranet, newsletter, emails and training sessions.

6 Monitoring and Review

Performance against Key Performance Indicators will be reviewed on an annual basis and used to inform the development of future procedural documents.

This policy will be reviewed on a every two years, and in accordance with the following on an as and when required basis:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

7 Legislation and related documents

A set of procedural document manuals will be available via the CCG/GMSS staff Intranet.

IG001 Information Governance Policy
IG002 Confidentiality and Data Protection Policy
IG003 Corporate Information Security Policy
IG004 Acceptable Use Policy (IT, Email and Internet)
IG005 Records Management Policy

IG006 Information Risk Policy
IG007 Information Governance Incident Reporting Procedure
IG008 Encryption Policy

Appendix 1: Audit Checklist

Date:
Service:
Number of Staff:

	Observations/Comments
Clear Desk	
Confidential Waste Disposal	
Working Paper in bins	
Locked Screens	
Unlocked filing cabinets (containing sensitive/personal info)	
Use of memory sticks	
Password Use – shared passwords	
Access to information/systems - controls in place - authorising access - audit	
Awareness of the Secure Transfer Procedure	
Awareness of reporting breach/incident concerning personal/business sensitive information	
Awareness of the Subject Access Procedures	
Other Observations	

Auditor Name	
Recommendations	
Follow up Actions	

Appendix 2 Non Compliance Observation Sheet

Department / Area:	**Audit Date:**
Details of Non-Compliance:	
Auditor Name:	**Signature:**
Recommendations:	
Follow Up Date:	**Additional Comments:**
Follow up / Action taken:	
Date Re-assessed:	
Auditor Name:	**Signature:**