Greater Manchester Shared Services

GMSS
Confidentiality Audit Procedure

Jan 2017

Greater Manchester Shared Services
Hosted by NHS Oldham CCG
on behalf of the Greater Manchester CCGs

Best Care • Best Health • Best Value

Document Change History

Date	Ver.	Status	Author	Details of Change
November 2016	0.1	Reviewed from Oldham CCG to fit GMSS	IG Team	Amendments to fit with GMSS

Document Tracking History

Date	Ver.	Person Presenting	Area Receiving	Comments
November 2016	0.1	IG Team	GMSS IG Group	Recommend Approval by the IG Group
January 2017	0.2	G Coxon	FPG	Recommend Approval after some amendments
January 2017	0.3	K Rigden	SMT	Amendments needed
February	1.0	K Rigden	SMT	Approved

Contents

1. Introduction 4
2. Purpose of a Confidentiality Audit 4
3. Responsibilities 4
4. Monitoring and Auditing Access to Confidential Information 5
5. Investigation Procedure and Responsibilities 7
6. Training and Awareness 9
7. Monitoring and Review 10
8. Legislation and Related Documents 10
9. Appendix 1: Audit Checklist 11

1. Introduction

This Procedure is a joint document written, approved and operational between NHS Oldham Clinical Commissioning Group (Oldham CCG) and its Informatics provider, NHS Greater Manchester Shared Service (GMSS).

Oldham CCG and GMSS are committed to a programme of effective risk and incident management. The 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 for or on behalf of GMSS such as third party contractors and others (e.g. business partners, including other public sector bodies, volunteers, commercial service providers) who may potentially use the GMSS facilities.

This procedure outlines the arrangements for the auditing and monitoring or privacy and confidentiality issues in relation to the processing of personal data. They provide 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. Purpose of a Confidentiality Audit

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 overall assurance framework.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfill 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 CCG sites
- Internal audits of reviews of IT security
- Complaints from members of the public / staff
- Informal alerts made by staff
- Reported near misses

3. Responsibilities

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. Recommendations and concerns arising from confidentiality audits are actioned within a reasonable timeframe.

The Information Governance Manager for GMSS and Senior Information Governance Officers for GMSS, 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.

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

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. This is documented in the Information Governance Incident Reporting Procedure.

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.

The Information Governance Group will be responsible for ensuring that the Confidentiality Audit Procedures are implemented throughout GMSS. This procedure will be approved by this Group.

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 Disciplinary Policy, up to and including, in appropriate circumstances, dismissal without notice.

All staff should be made aware that Information Governance audits around departments may occur at any time.

4. Monitoring and Auditing Access to Confidential Information

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 may be carried out by the Information Governance Team or with the Caldicott Guardians express written permission, the Information Asset Owner, 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 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 GMSS's incident reporting processes in order that the incident can be scored and action taken to prevent further breaches. Further information regarding this can be found in the Information Governance Incident Reporting Procedures.

The Information Governance Department will be responsible for ensuring that the Caldicott Guardian and / or SIRO are 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 with the requirements detailed in the Disciplinary Policy.

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 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).

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 as highlighted in the appendix will be used and undertaken by the Information Governance Department on an annual basis or more frequently where this is required. Staff must be aware that Information Governance audits may occur at any time. 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 1) and fed back to Heads of Department / Information Asset Owners for action and follow up. Areas of good practice will also be identified. This provides information as to their compliance with confidentiality requirements. Where non-compliance / information risks are observed, this needs to be reported back as soon as possible to the department / ward. Each non-compliance observed should have an associated risk assessment and recommendation for improvement addressed to the Head of Department or equivalent. 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. Further checks will be made to ensure the recommendation has been implemented and risks mitigated.

A formal report will also be produced detailing the outcome and any information risks identified. This will be presented to the Information Governance Group and the Caldicott / SIRO immediately 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 patient 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 / Heads of Departments 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 the Information Governance Department immediately so this can be followed up. It must be reported using the incident reporting procedures and following the Information Governance Incident Reporting processes.

Logging and Reporting of Confidentiality alerts / incidents / complaints.

All confidentiality alerts/incidents must be logged on GMSS DATIX system. Staff must also report them to the Information Governance Department where they will be logged on the Information Governance Incident Logbook. This also contains actions taken and lessons learned. Reports will be presented to the Information Governance Group and to the SIRO / Caldicott Guardian immediately where required. Lessons learned will be disseminated through appropriate communication processes as highlighted in the Information Governance Communications Strategy.

5. Investigation Procedure and Responsibilities

Confidentiality breaches may be reported via a different number of methods and to different

departments initially depending on the nature of the breach. The example below highlights the investigation process and responsibilities of each department involved.

The departments where breaches of confidentiality may be reported to include:

- Information Governance (for all breaches)
- Patient Services / Effective Use of Resources Team (concerning official complaints from patients / staff / public)
- People Services (if a breach of confidentiality has been alleged against a member of staff)

If the actual or suspected breach is reported to any department other than the Information Governance Department, it is important that this is forwarded to the Information Governance Department as soon as possible in order to co-ordinate the investigation in conjunction with the departments listed above. The alert / incident / complaint is officially logged on the Information Governance Incident and Complaints Log and an investigation is undertaken.

Responsibility of Patient Services / Effective Use of Resources Team.

Official complaints from patients / staff / public regarding confidentiality will mainly be received by the Patient Services and / or the Effective Use of Resources teams. On receipt of such a complaint, Patient Services and / or the Effective Use of Resources team follow their procedures regarding acknowledgement. The complaint should then be forwarded to the appropriate department for them to appoint a case manager to investigate and a copy sent to the Information Governance Department. The Case Manager should liaise with Information Governance regarding the investigation, action taken and lessons learned. The Case Manager must put together the formal response to send back to the complainant in conjunction with the Information Governance Department. Liaison with People Services will be made where appropriate.

Responsibility of the People Services.

Alerts over breaches of confidentiality by staff may be received directly to People Services and in these cases, People Services will inform the Information Governance Department so that these incidents can be logged on the Information Governance Incident logbook. Where it is suspected that a member of staff has deliberately misused or breached patient and / or staff confidentiality, People Services will co-ordinate the initial fact finding into the incident. This is to establish if there is any primia facia evidence to support the breach of confidentiality allegation.

If the initial fact finding suggests that there is primia facia evidence to support the allegation of breach of confidentiality the staff member will be informed and the People Services will appoint an independent Investigating Officer to undertake a full investigation in line with the requirements of the GMSS's Disciplinary Procedure.

Following completion of disciplinary proceedings feedback on any IG lessons learned will be given to the Information Governance Department. This is to enable key lessons learned to be disseminated to staff and to incorporate into training materials in order to mitigate information risk. Key IG lessons learnt will also be reported to all relevant committees/Governing Body meeting and escalated to SIRO / Caldicott Guardian escalation is required Confidentiality of individuals involved in disciplinary proceedings will be maintained and only summary lessons learnt will be disseminated that do not identify any individuals.

Responsibility of the Information Governance Group.

Any confidentiality breach / incident / complaint or alert must be reported to the Information Governance team in all cases and logged on the DATIX system. This will be recorded onto the Information Governance Incident and Complaints Logbook. All alerts / breaches / complaints will be treated as incidents according to the Information Governance Incident Reporting Procedures and scored accordingly as per the classification set out in the Checklist for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (Department of Health, June 2013). These will be located on the Intranet under Governance and Risk.

The Information Governance staff are responsible for undertaking confidentiality audits around the site to ensure procedures are being complied with. Staff are encouraged to report confidentiality alerts and possible breaches to the Information Governance Department. The area / department can then be investigated and reported to the Head of Department / Information Asset Owner.

If the incident relates to inappropriate access to an IT system, the Information Governance Department will inform People Services who will liaise with the relevant Information Asset Administrator / System Manager to produce an audit trail report. Please note this can only be undertaken for electronic record systems.

The Information Governance Department do not have access to any information systems containing personal confidential data and therefore cannot produce audit reports.

The Information Governance Department's role is to assist other departments regarding investigation of a breach and to ensure action is put in place to mitigate the risk by the department themselves and the GMSS as a whole via dissemination methods. This will be reported within the Information Governance Incidents and Complaints Logbook and regularly reported to the Information Governance Committee.

The Information Governance Department will disseminate lessons learned from alerts / incidents and complaints through appropriate communication processes as outlined in the Information Governance Communications Strategy.

The Information Governance Department will ensure that exceptional issues / breaches are escalated to the Caldicott Guardian and the SIRO for action and guidance.

It is not the Information Governance Department role to undertake reports / actions plans and root cause analysis for breaches / incidents reported. This is the responsibility of the Head of Department / Information Asset Owner / Investigating Officer from the department where the incident / alert has originated from. The Information Governance Department will assist and provide advice and guidance to these colleagues.

6. Training and Awareness

This procedure will be made available to all staff in the All Staff Folders. Staff are also informed about the reporting of breaches / alerts / incidents during 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 GMSS.

The Caldicott Guardian / SIRO 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.

7. Monitoring and Review

This procedure will be reviewed 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.

8. Legislation and Related Documents

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings.

9. Appendix 1: Audit Checklist

No.	Check	Findings			Recommended Improvements	Responsible	Deadline
		Yes / No/ Comments	RAG	Comments			
Physical Security							
1	Security pass required to enter floor / Wearing ID Badge						
2	Doors, Windows and locking systems						
3	Visitors supervised						
4	Restricted access areas						
5	Filing cabinets kept locked						
Computing Systems							
6	Password access required						
7	Are passwords known by others?						
8	Computer screens kept locked when away from desk?						
9	Can sensitive information on screen be seen by members of the public / non-authorised staff?						
10	Access to folders restricted?						
11	USB ports disabled?						

12	Are all laptops encrypted?						
13	Is any personal / sensitive data kept on the laptop desktop?						
14	Email - how is personal / sensitive data emailed						
15	Smartcards are not left in computer when away from desk?						
Filing							
16	Are cabinets lockable						
17	Where are keys stored						
18	Who has access to filing cabinets						
19	Is clear desk processes followed?						
20	Is any personal / sensitive data left out in office?						
Staff Awareness							
21	Undertaken IG Mandatory training?						
22	Know where staff guidance is?						
23	Know who IG Team are?						
24	Know who SIRO is?						

25	Know who Caldicott Guardian is?						
26	Who would you contact for support?						
27	Know how to log an IG incident?						
Confidential Waste Processes							
28	Use a cross cut shredder / confidential waste bin?						
Safe Haven							
29	Are post trays located in secure area?						
30	Are faxes used?						
31	If faxes are used are these safe haven faxes						
32	Any other observations?						
Signed by: (IG Team Carrying Out The Audit)		**Date:**					

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: