Bolton Clinical Commissioning Group

Confidentiality Audit Procedure

Policy Number	**IG009**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**17th September 2020**
Last Review Date	**April 2020**
Next Review Date	**17th September 2022**
Policy Author	**IG Team**
Version Number	**V4.1**

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
3.1	September 2018	GMSS IG Team	Updated to reflect GDPR, the Data Protection Act 2018 and DSP Toolkit
3.2	October 2018	IG Board	Approved
4.0	December 2018	Chief Officer	Approved
4.1	April 2020	IG Team	Reviewed

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

Contents

1 Introduction

Bolton Clinical Commissioning Group (thereafter known as the CCG) is committed to a programme of effective information risk and incident management incorporating data security, protection and confidentiality. Access to personal confidential information must be in accordance with Data Protection legislation, more specifically the General Data Protection Regulation (GDPR) principles and within the jurisdictions permitted for a CCG.

The GDPR is a legal framework that protects individual's personal data. In order for CCG staff to process this type of information they must a legal basis as per GDPR and be on a need to know basis, justified when required and monitored. The CCG are therefore required to regularly review how CCG staff process personal data.

This procedure outlines the arrangements adopted by the CCG for the auditing and monitoring of data security, protection 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 concerns are highlighted together with recommendations to ensure confidentiality is maintained.

The CCG has a procedure for investigating personal data breaches of data security and confidentiality as documented in the Data Security and Protection and Incident Reporting Procedure.

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

2 Aims and Objectives

Data security, protection and confidentiality audits will focus on control within electronic records management systems, paper record systems and data security and confidentiality processes undertaken by departments, for example checking transfers of information processes and housekeeping such as screen locking. The purpose is to discover whether data security and / or confidentiality has been breached or put at risk through deliberate or perhaps unknown 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 information risk assurance framework. Failure to ensure that adequate controls to manage and safeguard data security and confidentiality are implemented may and fulfil their intended purpose may result in a breach of that confidentiality. This potentially could contravene the requirements of Caldicott Principles, the General Data Protection Regulation (GDPR), the

Data Protection Act 2018, the Computer Misuse Act 1990 and the Human Rights Act 1998.

The following are typical data security and confidentiality alerts which are regularly monitored – please note this list is not exhaustive:

- Monitoring of data security / Information Governance (IG) personal data breaches and recommendations to ensure these are implemented Confidential (walk around) audits around the sites where Bolton CCG staff are located
- Complaints from members of the public / staff regarding processing of personal data
- Informal alerts made by staff
- Reported near misses

3 The General Data Protection Regulation (GDPR) Principles

Data Security, protection and confidentiality audit processes ensure that the CCG is adhering to the GDPR. The GDPR sets out seven principles (Article 5) which must be adhered to make sure the processing of personal data is lawful, they are:

Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
c) Adequate, relevant and limited to what is necessary
d) Accurate and kept up to date
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) Processed in a manner that ensures appropriate security of the personal data

And,

The controller shall be responsible for and be able to demonstrate compliance with the principles above

The CCG is a data controller.

The audit processes documented in this procedure provide evidence and assurance that the CCG is complying with the GDPR.

4 Definitions

General Data Protection Regulation 2016 (GDPR)

The GDPR is Data Protection legislation. The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of personal data.

Data Controller

A data controller determines the purposes and means of processing personal data.

Processing

This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data

This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Business Sensitive Information

This is information that if disclosed could harm or damage the reputation or image of an organisation.

Personal Data Breach

As per Article 4(12) of the GDPR, a “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Information Risk

An identified risk to any information asset that the CCG holds. Please see the Information Risk Policy for further information.

5 Roles and Responsibilities

Chief Operating Officer

The Chief Operating Officer has ultimate responsibility for the implementation of the provisions of this procedure. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support the safe and secure keeping of all personal data the CCG processes.

Caldicott Guardian

The Caldicott Guardian has overall responsibility for the monitoring incidents and complaints relating to confidentiality breaches which concern patient data and is responsible for ensuring that access to confidential patient information is regularly audited within the CCG. When necessary they are provided with recommendations arising from confidentiality audits, with timeframes and actions that have been taken.

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 CCG. Where information risks are identified these will be presented to the SIRO along with an action plan.

Data Protection Officer (DPO)

The DPO is responsible for advising on compliance including ensuring confidentially procedures are in place, provision of data security training and awareness and is also the main point of contact with the Information Commissioner.

The DPO will provide advice and guidance on any areas of concern that arise from the audits. They will ensure that action plans are implemented and completed.

Information Governance (IG) Team

The Information Governance Team are responsible for co-ordinating the approach for investigating data security and confidentiality alerts which arise from incidents, complaints, audit reports, informal alerts. The IG Team will provide a comprehensive audit report from their findings. This will be circulated to the CCG's IG Board and any other relevant IG members of staff (as above).

Information Asset Owners (IAO)

The Information Asset Owners (IAOs) support the SIRO and will support the IG team when areas of concern relating to information risk are identified within their department.

Line Managers

All managers are responsible for ensuring that staff for whom they are responsible for are aware of their responsibilities with regard to data security and confidentiality of information and ensure that staff complete the Data Security Awareness training.

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

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

Access to electronic and / or paper 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 electronic and / or paper confidential records in order that only those individuals with a legitimate right are given access. This authorisation must be documented and retained for monitoring purposes. This must also be documented in the Information Asset Register and include information as to who has gained access (name, title, department), the reason access required and the level of access permitted.

Information Governance Board

The Information Governance Board, chaired DPO is responsible for ensuring that the Confidentiality Audit Procedures are implemented throughout the CCG. The procedure will be reviewed and approved by this Board. This Board will receive Confidentiality Audit reports produced by the IG Team which aim to demonstrate how the CCG are complying with their GDPR responsibilities and obligations. This Board is able to escalate any concerns to the CCG's Executive Team.

All Staff

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

It is recognised that as a commissioning organisation the CCG do not process much personal data. There are certain departments i.e. NHS Funded Care team that have a legal right to. The majority of staff process information that can be classed as confidential to the organisation or business sensitive. This information should be treated in the same way as personal data.

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 Data Security / Information Governance audits may occur at any time without prior notice.

6 Monitoring and Auditing 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 basis.

Monitoring should be carried out by the Information Asset Owner or delegated to the Information Asset Manager / Administrator for an electronic system in order to check irregularities regarding access to confidential information can be identified. If irregularities are found these should be reported to the Data Protection Officer / Caldicott Guardian / SIRO and the IG Team following the CCG's incident reporting processes and action taken by the Information Asset Owner / 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 IG Team and logged as an incident following CCG's IG reporting processes in order that the incident can be reviewed and remedial action taken to mitigate further breaches. Further information regarding this can be found in the Data Security and Protection and Incident Reporting Procedure (IG007).

The IG Team are responsible for ensuring that the Data Protection Officer / Caldicott Guardian and / or SIRO are informed of any concerns highlighted as a result of monitoring compliance with data security and confidentiality processes.

If any member of staff fails to adhere to data security and confidentiality processes this will be dealt with in accordance the CCG's Disciplinary Policy.

Confidentiality audits will be conducted by the IG team on an annual basis, and will cover the following areas:

- Audit and observations of any data security, 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 / archiving procedures
- The location of post trays for incoming and outgoing mail – are they located in secure areas
- Staff comprehension regarding their responsibilities pertaining to data security and confidentiality and the rights regarding access to confidential information
- Checks to test staff awareness regarding:
    - Right of Access / Subject Access requests
    - Freedom of Information requests
    - how to report data security / IG incidents
    - who are the key IG contacts
    - what is personal data and a personal data breach
- Observations of good practice regarding assuring the data security and confidentiality of personal data and business sensitive data.

Methodology

Confidentiality audit checks are undertaken using a variety of methods such as unannounced spot checks and walk round site audits conducted by the DPO and IG Team and also using the methods as listed in Appendix A. The results of the walkabout audits and formal audits are discussed at the IG Board and any non-compliance will be followed up.

Areas of non compliance will be reported on the Non-Compliance Observation Sheet (Appendix B) 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 and / or 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 (such as Line Manager / Information Asset Owner) 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.

Reports will also be produced detailing the outcome and any information risks identified. These will be presented to the IG Board and when required to the Caldicott Guardian and / or SIRO.

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

Information Asset Owners / Line Managers must ensure that the use of the system / asset is monitored and check for any inappropriate activity such as failed login attempts or breaches of confidentiality.

The Data Security & Protection Toolkit (DSPT), which is completed annually to demonstrate the CCG's compliance to the GDPR, may contain staff survey questions, when provided, the IG Team will ensure the survey is circulated to the CCG to assess IG comprehension. This assists to highlight areas of good practice and identify areas where further training / guidance / support are required.

Logging and Reporting of confidentiality alerts/incidents

The CCG's Data Security and Protection and Incident Reporting Procedure (IG007) applies when any data security breach or IG incident needs to be reported. This is logged on the CCG Data Security Breaches / Information Governance Incident Reporting Logbook. The DPO and the IG Team will investigate and ensure they are reported to the ICO if required, via the Data Security and Protection Toolkit (DSPT).

Incident / data breach outcome reports will be submitted to the IG Board and to the DPO / Caldicott Guardian and SIRO. Exceptional issues will be escalated to the Caldicott Guardian and DPO for advice. Lessons learned will be disseminated through appropriate communication processes.

7 Training and Awareness

This procedure will be available on the CCG Intranet. Staff are also informed about the reporting of breaches / alerts / incidents via the CCG induction process. 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 staff.

The DPO / Caldicott Guardian and 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 data security / information governance related incidents via a variety of communication methods such as staff bulletins, policies, procedures, specific training etc.

8 Monitoring and Review

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.

9 Legislation and related documents

A set of procedural document manuals will be available via the CCG's website.

A number of other policies are related to this policy and all employees should be aware of this range below:

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 Data Security and Protection and Incident Reporting Procedure

Legal Acts:

- Data Protection Act 2018
- General Data Protection Regulation
- Human Rights Act
- Freedom of Information Act 2000
- Thefts Act (1968 and 1978)
- Police and Criminal Evidence Act 1984 (PACE)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

Appendix A - Data Security / Confidentiality Audit Pro Forma (walk around on site audit)

Detail of check	Tick if applicable	Comments	Improvements – Suggested improvements (if applicable)	Date Completed
Filing cabinets locked when not in use?				
Pass required entering the building?				
Reception manned?				
Visitors supervised?				
Doors / windows locked?				
Filing cabinets locked when not in use?				
Computer / laptop screen locked when away from desk?				
Are Smartcards / ID cards left unattended?				
Are cabinets lockable if contain Personal Data / Business Sensitive data?				
Is access restricted where filing cabinets contain Personal Data?				
Is a clear desk policy followed?				
PCD / business sensitive data left out on desks when unattended?				
Paperwork left on the printer				
Any Additional Comments				

Audit completed by …….. **Date …….**

Appendix B - 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:**