NHS
Bury
Clinical Commissioning Group

Confidentiality Audit Procedure

Version:	5.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Steering Group
Date ratified:	18 June 2021
Name of originator /author (s):	GMSS Information Governance Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	July 2021
Review date:	March 2023
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Confidentiality Audit Procedure CCG.GOV.025.5.1
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Information Governance Manager
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff.
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Information Governance Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place Knowsley Street Bury BL9 0SN Tel: 0161 762 1500
Copies of this document are available from	CCG Corporate Office CCG Website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
1.0 = Policy once ratified	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	27th November 2014
2.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	18th November 2015
2.1 = policy review	GMSS IG Team	25th August 2017
3.0 = Policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	19th September 2017
3.1 = policy review	GMSS IG Team	24th September 2018
4.0 = Policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	31st October 2018
4.1 = policy review	IG Team	15th June 2021
5.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Steering Group	18th June 2021

Confidentiality Audit Procedure

Contents

1. Introduction

1.1 Bury Clinical Commissioning Group (thereafter known as the CCG) are committed to a programme of effective risk and incident management incorporating data security, protection and confidentiality. Access to confidential information must be in accordance with the UK General Data Protection Regulation (UK GDPR) principles and within the jurisdictions permitted for a CCG. Therefore access must have a legal basis as per UK GDPR and be on a need to know basis, justified when required and monitored. The CCG has a procedure for investigating breaches of data security and confidentiality as documented in the Data Security and Protection and Incident Reporting Procedure.

1.2 This procedure applies to all CCG staff who for, or 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) who may potentially use the organisation's facilities.

1.3 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 concern highlighted together with recommendations to ensure confidentiality is maintained.

2. Purpose of a Confidentiality Audit

2.1 Data security, protection and cconfidentiality 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. The purpose is to discover whether data security and / or confidentiality has been breached or put at risk through deliberate misuse of systems as a result of weak, non-existent or poorly applied controls.

2.2 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 and fulfil their intended purpose may result in a breach of that confidentiality. This potentially could contravene the requirements of Caldicott, the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, the Computer Misuse Act 1990, the Human Rights Act 1998 and the Confidentiality Code of Conduct.

2.3 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) breaches and recommendations to ensure these are implemented;
- Confidential (walkaround) audits around the sites where Bury CCG staff are located;
- Complaints from members of the public / staff regarding processing of personal data;
- Informal alerts made by staff; and
- Reported near misses.

3. UK General Data Protection Regulation Principles (UK GDPR)

3.1 Data Security, protection and confidentiality audit processes ensure that the CCG is adhering to the UK GDPR principles (Article 5) when processing personal data which sets out that personal data should be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and kept up to date;
- 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; and
- Processed in a manner that ensures appropriate security of the personal data.

3.2 In addition, the CCG as data controller is responsible for and be able to demonstrate compliance with the principles above.

3.3 The audit processes documented in this procedure provide evidence and assurance that UK GDPR is being complied with and this can be demonstrated.

4. Roles and Responsibilities

4.1 The following roles and responsibility apply in respect to this policy:

- **Data Protection Officer (DPO)**

4.2 The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the UK GDPR and other data protection laws. They are required to monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

- **Caldicott Guardian**

4.3 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.

- **Senior Information Risk Owner (SIRO)**

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

- **Managers / Heads of Department / Information Asset Owners**

4.5 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 Data Security Awareness / Information Governance training.;

- 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 Policy and Procedure located on the CCG's website;
- complying with data security / confidentiality audits and ensuring that subsequent recommendations are complied with within specified timescales.
- Ensuring that access to electronic and / or paper confidential information is strictly controlled within each managers / information asset owner's area of responsibility;
- 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; and
- ensuring that any authorised access to confidential records is documented and retained for monitoring purposes, including in the Information Asset Register and should include as a minimum information as to who has gained access (name, title, department) the reason access required and the level of access permitted.

- **CCG IG Manager**

4.6 The CCG's Information Manager is responsible for day to day running of all information governance / data protection related activities in the CCG.

- **Information Governance Steering Group**

4.7 The Information Governance Steering Group is responsible for ensuring that the Confidentiality Audit Procedures are approved and subsequently implemented throughout the CCG.

- **Employees**

4.8 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.

4.9 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.

4.10 All staff should note that Data Security / Information Governance audits may occur at any time without any prior notice.

5. Monitoring and Auditing Access to Confidential Information

5.1 The following arrangements will apply in respect to this policy:

- **Monitoring**

5.2 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.

5.3 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 notified to the Data Protection Officer / Caldicott Guardian / CCG IG manager / GMSS IT Team and action taken by the Information Asset Owner / Manager / Administrator to rectify the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

5.4 Actual or potential breaches of confidentiality should be reported **immediately** to the IG Manager and logged as an incident, in line with the CCG's IG incident 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 Policy and Procedure.

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

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

- **Audits**

5.7 Confidentiality audits will be conducted by the IG Manager in conjunction with IG Staff Surveys 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 safe haven secure areas;
- Staff comprehension regarding their responsibilities pertaining to data security and confidentiality and the rights regarding access to confidential information;
- Checks to ensure staff have read, understood and signed the Confidentiality Code of Conduct / have an employment contract with relevant UK GDPR 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 data security / IG incidents; and
- Observations of good practice regarding assuring the data security and confidentiality of personal data and business sensitive data.

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

5.8 Areas of non- compliance will be reported on the Non-Compliance Observation Sheet (Appendix B) 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.

5.9 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.

5.10 A formal report will also be produced detailing the outcome and any information risks identified. This will be presented to the Information Governance Steering Group and Data Protection Officer / the Caldicott / SIRO immediately when applicable for escalation.

5.11 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.

5.12 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.

5.13 The IG Manager will undertake an annual staff survey to test comprehension using questions derived from the Data Security & Protection Toolkit (DSPT). This assists to highlight areas of good practice and identify areas where further training / guidance / support is required.

6. Training and Awareness

6.1 This procedure will be made available to all staff on the CCG's People matters portal, via the Corporate Office or on the CCG's website. Staff will also be informed about the reporting of breaches / alerts / incidents during via mandatory training and induction pack. 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.

6.2 The Data Protection Officer / Caldicott Guardian / SIRO and CCG IG Lead are made aware of information governance related incidents / complaints / alerts reported and the associated action plans to mitigate similar incidents occurring in the future.

6.3 All staff will continue to be informed about the importance of reporting data security / information governance related incidents via a variety of media such as staff bulletins, policies and procedures, emails and specific training.

7. Monitoring and Review

7.1 This policy 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. Equality Assessment Impact

8.1 The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, service users and the public have been reviewed in line with the CCG Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, service users and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/ belief

9. Legislation and Related Documents

9.1 This document should be read alongside the suite of Information Governance and Data Protection policies, including, but not limited to:

- Information Governance Framework
- Data Protection Policy
- Records management Policy
- Information Risk Policy
- Information Governance Incident Reporting Policy
- Confidentiality Code of Conduct

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:**