NHS
Bury
Clinical Commissioning Group

Confidentiality Audit Procedure

Version:	4.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date ratified:	31st October 2018
Name of originator /author (s):	Information Governance Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	November 2018
Review date:	November 2020
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.025.4.0
Category of Document in The Policy Schedule	Governance
Author(s) **Contact(s) for further information about this document**	Information Governance Team
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 Operational 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	NHS Bury Clinical Commissioning Group,	19th September 2017

ratified	Information Governance Operational Group	
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

Confidentiality Audit Procedure

Table of Contents

1. Introduction **4**
2. Purpose of a Confidentiality Audit **4**
3. General Data Protection Regulation Principles (GDPR) **5**
4. Roles and Responsibilities **5**
5. Monitoring and Auditing Access to Confidential Information **7**
6. Training and Awareness..**9**
7. Monitoring and Review...**9**
8. Equality Assessment Impact **9**
9. Legislation and Related Documents...**9**
Appendix A : Data Security / Confidentiality Audit Pro Forma (walk around on site audit).......**11**
Appendix B - Non Compliance Observation Sheet...**12**

1. Introduction

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 General Data Protection Regulation (GDPR) principles and within the jurisdictions permitted for a CCG. Therefore access must have a legal basis as per 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.

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.

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

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.

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 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.

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
- Reported near misses

3. General Data Protection Regulation Principles (GDPR)

Data Security, protection and confidentiality audit processes ensure that the CCG is adhering to the GDPR principles (Article 5) when processing personal data which are as follows:

Personal data shall be:

1a) Processed lawfully, fairly and in a transparent manner
1b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
1c) Adequate, relevant and limited to what is necessary
1d) Accurate and kept up to date
1e) 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
1f) Processed in a manner that ensures appropriate security of the personal data

And,

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

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

4. Roles and Responsibilities

Responsibility of the Data Protection Officer (DPO)

The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the 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).

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

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 the CCG.

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 data security and confidentiality of information and ensure that staff complete Data Security Awareness / Information Governance 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 Policy and Procedure located on the CCG's website.

They are also responsible for complying with data security / 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 should include information as to who has gained access (name, title, department) the reason access required and the level of access permitted.

Responsibility of the GMSS IG Team

The GMSS Information Governance (IG) Team, are responsible for co-ordinating the approach for investigating data security and confidentiality alerts which arise from incidents, complaints, audit reports, informal alerts.

Responsibility of the Information Governance Operational Group

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

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

All staff should be made aware that Data Security / Information Governance audits may occur at any time without any prior notice.

5. 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 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 / CCG IG Lead / GMSS IG Team 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 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.

The IG Team will be responsible for ensuring that the Data Protection Officer / Caldicott Guardian / SIRO and / or CCG IG Lead 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 with the requirements detailed in the CCG's Disciplinary Policy.

Confidentiality audits will be conducted by the IG team 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 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
- 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, SIRO 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 Operational Group 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 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 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.

A formal report will also be produced detailing the outcome and any information risks identified. This will be presented to the Information Governance Operational Group and Data Protection Officer / 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 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 IG Team 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.

Logging and~~,~~ Reporting of Confidentiality Alerts / Incidents

The CCG’s Data Security and Protection and Incident Reporting Policy and Procedure 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 Information Governance Operational Group and to the Data Protection Officer / Caldicott Guardian / SIRO and CCG IG Lead. The reports will detail actions taken and lessons learned. Exceptional issues will be escalated to the Data Protection Officer and Caldicott Guardian for advice. Lessons learned will be disseminated through appropriate communication processes.

6. Training and Awareness

This procedure will be made available to all staff on the CCG's website. Staff are also informed about the reporting of breaches / alerts / incidents during via mandatory training and induction. 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 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.

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

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

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

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

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

All documents in the CCG Policies and Procedures Register are relevant.

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:**