Confidentiality Audit Procedure

Responsible Officer:	SIRO, Deputy Chief Officer
Author:	Senior IG Specialist, eMBED
Date Approved:	12th February 2018
Committee:	Audit & Governance Committees
Version:	2.0
Review Date:	February 2021

CCGs working together

Airedale, Wharfedale and Craven CCG
Bradford City CCG
Bradford Districts CCG

Contents

1. Introduction

This document defines the procedure for carrying out audits relating to access to personal confidential data for NHS Airedale, Wharfedale and Craven Clinical Commissioning Group, NHS Bradford City Clinical Commissioning Group and NHS Bradford Districts Clinical Commissioning Group (hereafter known as the CCGs).

The purpose of this procedure is to ensure that staff only access the records of patients with whom they have a legitimate relationship, or in the case of all Personal Confidential Data (PCD), a sound legal basis and a legitimate business reason. It also helps ensure the organisation meets the requirements of the NHS Care Record Guarantee, the Information Governance Toolkit (IGT), Data Protection Act, and the General Data Protection Regulation.

2. Purpose

The purpose of confidentiality audits is to ensure that only appropriate staff access personal confidential data. In order to;

- Preserve Integrity:
  Protect information held on the organisation's network from unauthorised or accidental modification

- Preserve Confidentiality:
  Protect the organisation's information against unauthorised disclosure

Due to the nature and duties of CCGs, the holding of patient information is expected to be limited. All Personal Confidential Data (PCD) flows are documented on the Data Flow Mapping (DFM) and are available as part of the Information Governance Toolkit (IGT).

3. Scope

The procedure applies to all staff who work for the CCGs (including those on temporary or honorary contracts, secondments, pool staff and students) and who have access to CCG systems which hold personal information. It also applies to relevant people who support and use these systems.

All accessible work areas within the CCGs will be subject to the confidentiality audit programme.

4. Accountability

4.1 Caldicott Guardian

The Caldicott Guardian will be responsible for ensuring that patient confidentiality is protected within the organisation and promotes patient confidentiality considerations at Governing Body level**.** The Caldicott Guardian is Michelle Turner, Director of Quality and Nursing.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is the Governing Body member responsible for maintaining oversight of the information risks of the organisation, including monitoring incidents and complaints relating to confidentiality breaches within the CCG. The SIRO is Julie Lawreniuk, Chief Financial Officer and Deputy Chief Officer.

4.3 Information Governance Lead

The Information Governance Lead is responsible for ensuring effective management, accountability, compliance and assurance for all aspects of IG and for liaising with the information governance team from Embed Health Consortium who provide agreed support to the CCGs. The senior level information governance (IG) lead for the CCGs, is Fiona Jeffrey, Associate Director of Corporate Affairs (supported by Sarah Dick, Head of Governance).

4.4 Audit and Governance Committees

The Audit and Governance Committees ensure that the appropriate policies, procedures and structures are developed and put in place to provide a robust governance framework for information management, thereby ensuring CCG compliance with the national Information Governance Toolkit requirements.

The Audit and Governance Committees will also be responsible for sharing common issues and ensuring that concerns and recommendations arising from confidentiality audits are actioned within a reasonable timescale.

4.5 Information Asset Owners

Information Asset Owners (IAOs) will be responsible for ensuring that staff are aware of their responsibilities with regard to confidentiality when accessing any personal confidential data within the systems that they (the IAO) is responsible for.

4.6 Line Managers

Line managers should ensure that all new starters successfully complete the appropriate information governance training on commencement and prior to accessing any confidential information.

They must also ensure that staff are aware of where to seek further guidance in relation to confidentiality and the mechanisms for reporting potential or actual breaches of confidentiality and the consequences regarding disciplinary processes.

5. Procedure

Confidentiality audits will focus primarily on controls within electronic information management systems (particularly those systems available to most/all staff); however this will not exclude paper record systems (on desks and unlocked pedestals, filing cabinets and storage areas, for example).

The audit will seek to determine whether confidentiality is being breached (by virtue of the investigator having access to data that they would otherwise not expected to have access to), put at risk through deliberate misuse of the system (with malicious intent), or as a result of weak, non-existent or poorly applied controls (unlocked storage of PCD).

The audit will look for staff awareness of CCG confidentiality and security processes, appropriate use of faxes and hard copy PCD and that exchanges of PCD that involve email are secure and the physical security of work areas.

The audit may focus on one particularly work area or system or seek to review the overall level of compliance for the organisation as detailed below.

5.1 Audit trails and regular security checks

Where staff or patient information is held within a computer system, the CCGs will arrange that, at least yearly, an audit trail will be run for a system holding personal confidential data.

5.2 Security checks for paper records or simple computer facilities

The minimum checks to be performed are:

- The information is held securely e.g. password control or physical security
- The list of those with legitimate access is up to date

5.3 Information to be contained in the audit trail

The information to be contained within the audit will contain at minimum the following information

- Failed attempts to access confidential information
- Repeated attempts to access confidential information
- Successful access of confidential information by unauthorised persons
- Evidence of shared logins

5.4 Information Governance Compliance checks

Information Governance Compliance checks around the office of the CCG will be carried out at regular intervals.

Areas to be audited may include:

- Security applied to manual files, e.g. storage in locked cabinets/locked rooms
- The existence and location of whiteboards containing confidential information
- The location of fax machines and answer phones which receive confidential information. Whether Safe Haven guidelines are being followed
- The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information
- Retention and disposal arrangements included confidential waste

6. Reporting

The findings of the confidentiality audit will be reported to the Head of Governance, Associate Director of Corporate Affairs, SIRO and Caldicott Guardian and action taken where necessary regarding the implementation of any controls or remedial action to address the situation.

The SIRO and/or the Caldicott Guardian will decide if further investigation should be carried out or disciplinary action taken.

The investigation and management of confidentiality incidents will be in line with the CCGs incident reporting policies, Data Protection Act, General Data Protection Regulation and the Health and Social Care Information Centre (HSCIC)/NHS Digital's Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Reports will be to the submitted to the Audit and Governance Committees on at least an annual basis highlighting findings from the confidentiality audits.

7. Training needs analysis

The findings of the audit may require individuals and teams to complete further IG training where specific risks have been identified that demonstrate poor awareness or understanding, particularly in those environments that handle PCD.

8. Implementation and dissemination

Following ratification by the Audit and Governance Committees this procedure will be disseminated to staff by email and made available for reference through local or public CCG web services.

This procedure will be reviewed every two years or in line with changes to relevant legislation or national guidance.

9. Public Sector Equality Duty

The Equality Act 2010 includes a general legal duty to:

- Eliminate unlawful discrimination, harassment victimisation and any other conduct prohibited under the Act
- Advance quality of opportunity between people who share a protected characteristic and people who do not share it
- Foster good relations between people who share a protected characteristic and people who do not have it

The protected characteristics are:

- Age
- Disability
- Gender reassignment

- Marriage or civil partnership
- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

Public bodies have to demonstrate due regard to the general duty. This means active consideration of equality must influence the decisions reached that will impact on patients, carers, communities and staff.

It is no longer a specific legal requirement to carry out an Equality Impact Assessment on all policies, procedures, practices and plans but, as described above, the CCGs do need to be able to demonstrate they have paid due regard to the general duty.

This procedure sets out how the CCGs ensure that information is managed legally, efficiently and effectively. It is not believed that this policy will impact on or affect differently or adversely any of the groups with protected characteristics.

10. Legal references

General Data Protection Regulations 2016
Health and Social Care (Safety and Quality) Act 2015
Health and Social Care Act 2012
Privacy and Electronic Communications Regulations 2003
The Health Service (Control of Patient Information) Regulations 2002
NHS Information Governance Guidance on Legal and Professional Obligations (legislation prior to 2007)