NHS
Harrogate and Rural District
Clinical Commissioning Group

Confidentiality Audit Policy

November 2017

Authorship:	**Information Governance Manager**
Committee Approved:	Audit Committee
Approved date:	November 2017
Review Date:	November 2020
Equality Impact Assessment:	Completed
Target Audience:	Council of Members, Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	051
Version Number:	3.0

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Barry Jackson	First draft for comments	NR	
1.0	Barry Jackson	Approved version		
2.0	Helen Sanderson	Review ahead of Scheduled Review in March 2016 – No Amendments required	IGSG Oct 2015	
3.0	IG Officer	Reflect changes in organisational relationships (CSU to Embed) Add requirements of the General Data Protection Regulation 2016	Audit Committee November 2017	January 2018

CONTENTS

1 INTRODUCTION AND APPLICABILITY

1.1. It is essential that Harrogate and Rural District Clinical Commissioning Group (The CCG) implement appropriate systems to ensure that personal confidential information and commercially sensitive information is held and processed in a confidential and secure manner. In order to ensure that appropriate controls are maintained the CCG must implement a system of reviews to assess controls in place and compliance to these controls.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

4 SCOPE

This policy requires that the CCG reviews both general controls in place within their departments to protect Personal Confidential Data (PCD) being processed, including within specific information systems, and map and review data flows on a regular basis. The responsibilities in respect of information confidentiality audits are as follows:

Caldicott Guardian

The Caldicott Guardian is responsible for monitoring incidents and complaints in relation to confidentiality breaches within the CCG. The Caldicott Guardian will receive reports of potential or actual incidents identified during the audits undertaken in order to monitor investigations as appropriate and ensure appropriate corrective action taken.

SIRO

The SIRO are both responsible for monitoring risks in relation to information security and should receive reports of audit results to monitor weaknesses identified and ensure corrective action is implemented

IG Lead

The CCG Information Governance Lead will co-ordinate with the Embed Information Governance Team to ensure a system of CCG departmental audits on an annual basis. These audits may involve some or all of the audit mechanisms detailed in section 5.2.

Head of Departments/ Team Leaders

Heads of Departments and Team Leaders will be responsible for ensuring that their staff are aware of their responsibilities with regard to confidentiality and information security. They must also staff understand how to report actual or potential confidentiality breaches.

Additionally Heads of Department and Team Leaders are responsible for ensuring that staff have completed their statutory and mandatory training and any additional training modules as appropriate to the staff members job role identified during staff appraisals.

They will be responsible for completing confidentiality audits as required and implementing recommended corrective actions identified within agreed timescales.

Information Asset Owners

Information Asset Owners (IAO's) are responsible for ensuring that access to PCD is secure and strictly controlled within their area.

IAO's must allow ensure that all information assets are recorded on the CCG information asset register and where these involve the processing of personal identifiable information the flow of data must be mapped and risk assessed on a timely basis

Access to PCD must be allocated on a strict need to know basis, by those who require that access in order to perform their duties, appropriate documented authorisation must be obtained to demonstrate the need to know prior to access being given.

Access to information assets must be monitored in particular where access is attempted where it has previously been denied.

IM &T Services

IM&T services will be responsible for ensuring that confidentiality audits relating to central IT systems are conducted and corrective actions are identified and implemented within agreed timescales.

All Staff

Staff should ensure that they comply with the access rights allocated to them and not attempt to exceed these rights.

Staff should also be aware that it is their duty to report potential weaknesses in information security and potential or actual breaches to confidentiality.

Staff will be responsible for complying with confidentiality audits conducted within their area and complying with agreed recommendations resultant from the audits

5 POLICY PURPOSE & AIMS

5.1 Purpose

Information Asset Owners, Departmental Heads and Team Leaders should monitor information security within their areas on a continual basis, in order that irregularities are identified and corrective action implemented.

All potential and actual breaches should be reported immediately via the corporate incident reporting system, and to the organisations Caldicott Guardian.

Additionally regular audits must be undertaken to review information security controls in place and compliance to these controls.

5.2 Mechanisms for Auditing Information Security Controls

The Information Governance Team will develop an audit plan to co-ordinate work as appropriate to ensure the following are undertaken as necessary.

a. **General Information Security/ Safe Haven Procedures**
   It is essential that all departments have appropriate information security controls in place to protect PCD at all times. The security and transmission of confidential information/ safe haven standard includes an audit checklist to enable IAO's and department heads to record the assessment of controls in place.

b. **Review of Information Asset Register and associated Data Flow Maps**
   Information asset owners must on a regular basis review their information asset register to ensure that all information assets are recorded and the associated information flow maps have been documented and risk assessed.

c. Review of Network Folders, Shared Mailbox and individual systems access.

Access of staff to network folders and shared mailboxes should be reviewed on a regular basis, to ensure that leavers have been removed and access allocated is appropriate to the job role. This will require reports of access levels to be produced via the IM&T department and departmental managers/team levels to review access levels set.

This process also needs to be undertaken for specific systems, to ensure that access is allocated to staff on a need to know basis and that all live users are current employees.

d. Failed Log-ins

Periodically and upon the suspicion of attempted unauthorised access to network folders or an individual system, checks should be made to assess whether unauthorised access has been attempted or obtained. The IM&T Department would need to assist in the production of reports enable these assessments to be undertaken.

e. Monitoring Incidents

All Information Security and Confidentiality incidents reported within 24 hours and must be monitored and investigated, advise and assistance should be obtained from the Information Governance Team this includes potential and actual incidents identified as a result of any audit work undertaken.

5.3 Audit Reporting and Follow-up

A formal report will be produced detailing the outcome of the audit, recommendations, corrective action and completion timescales agreed.
These reports must be provided to both the Caldicott Guardian and the SIRO for monitoring purposes.

Arrangements should be made to follow-up corrective action agreed to ensure appropriate implementation and that where necessary system documentation and procedures are amended accordingly.

All risks identified must be reported as appropriate on the corporate risk register until such a time as appropriate corrective action is complete. All residual risks must remain on the corporate risk register for management consideration.

5.4 Audit Closure

Once the corrective action has been implemented and checked the audit can be formally closed.

6 IMPLEMENTATION

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

7 TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet.

8 MONITORING & AUDIT

Adherence to this policy will be monitored on an on-going basis and breaches may result in disciplinary procedures.

9 POLICY REVIEW

This policy will be reviewed in three years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

Appendix 1

1. Equality Impact Analysis	
Policy / Project / Function:	Confidentiality Audit Policy
Date of Analysis:	13/01/14
This Equality Impact Analysis was completed by: (Name and Department)	C Wallace - IG Manager – CSU IG Team
What are the aims and intended effects of this policy, project or function ?	This document sets out the need and the process for reviewing access to confidential data that the CCG holds.
Please list any other policies that are related to or referred to as part of this analysis?	
Who does the policy, project or function affect ? Please Tick ✔	Employees ☒ Service Users ☐ Members of the Public ☐ Other (List Below) ☐

2. **Equality Impact Analysis: Screening**					
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact
	Yes	No	Yes	No	
Race	☐	☒	☐	☒	
Age	☐	☒	☐	☒	
Sexual Orientation	☐	☒	☐	☒	
Disabled People	☐	☒	☐	☒	
Gender	☐	☒	☐	☒	
Transgender People	☐	☒	☐	☒	
Pregnancy and Maternity	☐	☒	☐	☒	
Marital Status	☐	☒	☐	☒	
Religion and Belief	☐	☒	☐	☒	
Reasoning					
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7					