Creating a healthier Hull

NHS Hull Clinical Commissioning Group

CONFIDENTIALITY AUDIT POLICY

September 2019

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Confidentiality Audit Policy
Date Issued:	October 2019
Date to be reviewed:	2 years after approval

Policy Title:	Confidentiality Audit Policy
Supersedes: (Please List)	Confidentiality Audit Policy
Description of Amendment(s):	Amendments to reflect the Data Protection Act 1998 (to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation). Removal of reference to DPA 98. Data Protection Impact Assessments Grammatical changes. Further IAO guidance.
This policy will impact on:	All Staff
Version No:	2.1
Issued By:	IG Team
Author:	IG Team
Effective Date:	November 2019
Review Date:	November 2021
Equality Impact Assessment Date:	October 2019

APPROVAL RECORD		**APPROVAL RECORD**
	Integrated Audit and Governance Committee	November 2019
Consultation:	Heads of Teams / IG Steering Group / Relevant Others	October 2019

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 and Date
0.1	Barry Jackson	First draft for comments	NR
1.0	Barry Jackson	Approved version	
1.1	C Wallace	Updated to new layout	8 March 2016
1.2	M Culling	Amendments to reflect the Data Protection Act 1998 (to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).	16 January 2018
2.0	Hayley Gilllingwater	Removal of reference to DPA 98. Data Protection Impact Assessments Grammatical changes. Further IAO guidance.	Integrated Audit and Governance Committee – 12 November 2019

CONTENTS

1 INTRODUCTION AND APPLICABILITY

1.1 It is essential that NHS Hull Clinical Commissioning Group (The CCG) implement appropriate systems to ensure that personal confidential information and commercially sensitive information is held and its legitimate processing during the course of bone fide CCG business is undertaken 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 the controls in place and compliance to these controls.

2 ENGAGEMENT

2.1 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 ANALYSIS

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

4.1 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:

i) 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.

ii) Senior Information Risk Officer (SIRO)

The SIRO is responsible for monitoring risks in relation to information security and receives reports of the audit results to monitor weaknesses identified and ensure corrective action is implemented.

iii) Data Protection Officer

Under the GDPR, public authorities or organisations that carry out large scale processing of sensitive data must appoint a Data Protection Officer (DPO). The role of the DPO is to facilitate the CCG's compliance with GDPR and they:

- Monitor CCG compliance with the GDPR
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments (DPIAs).
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
- Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, data protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches.

iv) Information Governance Lead

The CCG Information Governance Lead will co-ordinate 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.

v) 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 also ensure that 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 member's job role or as identified during staff appraisals.

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

vi) Information Asset Owners

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

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 and, in particular, where access is attempted where it has previously been denied.

vii) IT Services

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

viii) All Staff

Staff should ensure that they comply with the access rights allocated to them and not attempt to exceed these rights. Staff should be aware that their access may be monitored.

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 AND 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 proactively 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.

i) 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.

ii) **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. The IAR is sent to IAOs to be updated on a quarterly basis, IAOs are required to respond to the request for updates even if there are no changes to their assets.

iii) **Review of Network Folders and individual systems access.**

Access for staff to sensitive or controlled network folders 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 IT 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.

iv) **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 IT Department would need to assist in the production of reports to enable these assessments to be undertaken.

v) **Monitoring Incidents**

All information security and confidentiality incidents reported must be monitored and investigated by 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 will be formally closed.

6 IMPLEMENTATION

The policy will be disseminated through publication on the CCG's website 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 AND AWARENESS

All staff are required to complete the appropriate level of information governance training in accordance with NHS England and CCG policy. This is monitored via the CCG's Personal Development Review process.

8 MONITORING AND EFFECTIVENESS

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

9 POLICY REVIEW

This policy will be reviewed every 2 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

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Confidentiality Audit Policy V1.2 DRAFT3
Date of Analysis:	07/12/17 Reviewed 17/09/2019
Completed by: **(Name and Department**)	Dr Mark Culling Reviewed by: Hayley Gillingwater IG Team
What are the aims and intended effects of this policy, project or function?	The overall purpose of the policy is to set out the CCG's approach to confidentiality audits within the workplace. The policy will also set out guidance to staff and managers about their responsibilities in relation confidentiality audits.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	No No significant changes following policy review.
Please list any other policies **that are related to or referred to as part of this analysis**	Safe Haven Policy v1.2 General Data Protection Regulation (GDPR) Data Protection Act 2018
Who will the policy, project or function affect?	Employees and the general public

What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Consultation on the new policy has taken place nationally and locally. Consultation on the updated policy has taken place locally.
Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs	The policy does not directly promote inclusivity but provides a framework for the CCG's approach to confidentiality audits within the workplace, ensuring staff are supported by management and health professionals

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function?	Yes ☑ No □
Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.*	Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact?
Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	**Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?

(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

Protected Characteristic:	**Neutral Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)**
Gender	X			This policy applies to all regardless of gender
Age	X			This policy applies to all regardless of age
Race / ethnicity / nationality	X			This policy applies to all staff regardless of race/ethnicity. Analysis of employee data indicates that the percentage of white employees is reflective of the local population. However, the proportion of BME staff is lower than that of the local population it serves All staff require

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

				competencies which include the ability to read and understand English or to request the information in another format available to them
Disability	X			This policy applies to all regardless of disability
Religion or Belief	X			This policy applies to all regardless of religion or belief
Sexual Orientation	X			This policy applies to all, regardless of sexual orientation
Pregnancy and Maternity	X			This policy applies to all regardless of pregnancy or maternity
Transgender / Gender reassignment	X			This policy applies to all regardless of transgender/gender reassignment
Marriage or civil partnership	X			This policy applies to all regardless of marriage or civil partnership

<table>
<tr><th colspan="5">Action Planning:</th></tr>
<tr><td colspan="5"><b>As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?</b></td></tr>
<tr><td><b>Identified Risk:</b></td><td><b>Recommended</b></td><td><b>Responsible</b></td><td><b>Completion</b></td><td><b>Review</b></td></tr>
</table>

	Actions:	**Lead:**	**Date:**	**Date:**
As the policy is written in English there is a potential impact on employees whose first language is not English and therefore may struggle reading the policy.	The CCGs internal ‘portal’ and external website signpost individuals to alternative formats such as large print, braille or another language.	CCG Communications	Updating of this facility is ongoing	Next Policy Review - November 2021

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan

If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:

Signed:

Date: 31.10.19