NHS
North Lincolnshire
Clinical Commissioning Group

Confidentiality Audit Policy

Authorship:	Information Governance Officer
Committee Approved:	Quality, Performance & Finance
Approved date:	8 March 2018
Review Date:	March 2018
Equality Impact Assessment **Sustainability Impact Assessment** **Target Audience:**	**Screening** **Completed** **All Staff**
Policy Reference No:	N/A
Version Number:	1.1

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		
1.1	Mark Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).		

CONTENTS

		Page
1	**Introduction & Applicability**	4
2	**Engagement**	4
3	**Impact Analyses** **3.1 Equality** **3.2 Sustainability** **3.3 Bribery Act 2010**	 4 4 4
4	**Scope**	5
5	**Policy Purpose and Aims**	6 - 7
6	**Implementation**	7
7	**Training and Awareness**	7
8	**Monitoring and Audit**	7
9	**Policy Review**	7
	Appendices – Appendix 1 – Equality Impact Analysis **Appendix 2 – Sustainability Impact Assessment**	9 - 16 17

1 INTRODUCTION AND APPLICABILITY

1.1. It is essential that North Lincolnshire 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.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

3.3 Bribery Act 2010

The Bribery Act is particularly relevant to this policy. Under the Bribery Act it is a criminal offence to:

- Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and
- Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.

These offences can be committed directly or by and through a third person and other related policies and documentation (as detailed on the CCG intranet) when considering whether to offer or accept gifts and hospitality and/or other incentives.

Anyone with concerns or reasonably held suspicions about potentially fraudulent activity or practice should refer to the Local Anti-Fraud and Corruption Policy and contact the Local Counter Fraud Specialist

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.

Data Protection Officer (from 25th May 2018)

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

- Monitor CCG compliance with the GDPR
- Provide advice and assistance with regards to the completion of Privacy Impact Assessments
- 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, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

IG Lead

The CCG Information Governance Lead will co-ordinate with the eMBED Health Consortium 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.

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 and individual systems access.**
   Access of staff to 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 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 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 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 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

1. Equality Impact Analysis	
Policy / Project / Function:	Confidentiality Audit Policy
Date of Analysis:	13/11/17
This Equality Impact Analysis was completed by: **(Name and Department)**	M Culling Senior IG Specialist – eMBED Health Consortium 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					

3. **Equality Impact Analysis: Local Profile Data**	
Local Profile/Demography of the Groups affected (population figures)	
General	
Age	
Race	
Sex	
Gender reassignment	
Disability	
Sexual Orientation	
Religion, faith and belief	
Marriage and civil partnership	
Pregnancy and maternity	

4. **Equality Impact Analysis: Equality Data Available**	
Is any Equality Data available relating to the use or implementation of this policy, project or function? 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'.* Examples of *Equality Data* include: (this list is not definitive) 1. Application success rates *Equality Groups* 2. Complaints by *Equality Groups* 3. Service usage and withdrawal of services by *Equality Groups* *4.* Grievances or decisions upheld and dismissed by *Equality Groups* 5. *Previous EIAs*	Yes ☐ No ☒ Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document).
List any Consultation e.g. with employees, service users, Unions or members of the public that has taken place in the development or implementation of this policy, project or function	
Promoting Inclusivity **How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation**	

5. Equality Impact Analysis: Assessment Test

What impact will the implementation of this policy, project or function have on employees, service users or other people who share characteristics protected by *The Equality Act 2010* ?

Protected Characteristic:	No Impact:	Positive Impact:	Negative Impact:	Evidence of impact and if applicable, justification where a *Genuine Determining Reason* exists
Gender (Men and Women)	X			
Race (All Racial Groups)	X			
Disability (Mental and Physical)	X			
Religion or Belief	X			
Sexual Orientation (Heterosexual, Homosexual and Bisexual)	X			

What impact will the implementation of this policy, project or function have on employees, service users or other people who share characteristics protected by *The Equality Act 2010* ?

Protected Characteristic:	No Impact:	Positive Impact:	Negative Impact:	Evidence of impact and if applicable, justification where a *Genuine Determining Reason* exists
Pregnancy and Maternity	X			
Transgender	X			
Marital Status	X			
Age	X			

6. Action Planning

As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse outcomes identified on employees, service users or other people who share characteristics protected by *The Equality Act 2010* ?

Identified Risk:	Recommended Actions:	Responsible Lead:	Completion Date:	Review Date:

7. Equality Impact Analysis Findings				
Analysis Rating:	□ Red	□ Red/Amber	□ Amber	□ **Green**

		Actions	Wording for Policy / Project / Function
Red **Stop and remove the policy**	**Red:** As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share *Protected Characteristics.* It is recommended that the use of the policy be suspended until further work or analysis is performed.	**Remove the policy** Complete the action plan above to identify the areas of discrimination and the work or actions which needs to be carried out to minimise the risk of discrimination.	No wording needed as policy is being removed
Red Amber **Continue the policy**	As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share *Protected Characteristics.* However, a genuine determining reason may exist that could legitimise or justify the use of this policy and further professional advice should be taken.	**The policy can be published with the EIA** List the justification of the discrimination and source the evidence (i.e. clinical need as advised by NICE). Consider if there are any potential actions which would reduce the risk of discrimination. Another EIA must be completed if the policy is changed, reviewed or if further discrimination is identified at a later date.	As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share *Protected Characteristics.* However, a genuine determining reason exists which justifies the use of this policy and further professional advice. ***[Insert what the discrimination is and the justification of the discrimination plus any actions which could help what reduce the risk]***

Equality Impact Findings (continued):		
	Actions	Wording for Policy / Project / Function

Amber **Adjust the Policy**	As a result of performing the analysis, it is evident that a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the actions detailed within the *Action Planning s*ection of this document.	**The policy can be published with the EIA** The policy can still be published but the Action Plan must be monitored to ensure that work is being carried out to remove or reduce the discrimination. Any changes identified and made to the service/policy/ strategy etc. should be included in the policy. Another EIA must be completed if the policy is changed, reviewed or if further discrimination is identified at a later date.	As a result of performing the analysis, it is evident that a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the actions detailed within the *Action Planning s*ection of this document. ***[Insert what the discrimination is and what work will be carried out to reduce/eliminate the risk]***
Green **No major change**	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.	**The policy can be published with the EIA** Another EIA must be completed if the policy is changed, reviewed or if any discrimination is identified at a later date	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.

Brief Summary/Further comments	

Approved By		
Job Title:	Name:	Date:

Appendix 2

SUSTAINABILITY IMPACT ASSESSMENT

Policy / Report / Service Plan / Project Title:				
Theme (Potential impacts of the activity)	**Positive Impact**	**Negative Impact**	**No specific impact**	**What will the impact be? If the impact is negative, how can it be mitigated? (action)**
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			X	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			x	
Reduce the risk of pollution and avoid any breaches in legislation.			x	
Goods and services are procured more sustainability.			x	
Reduce carbon emissions from road vehicles.			x	
Reduce water consumption by 25% by 2020.			x	
Ensure legal compliance with waste legislation.			x	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			x	
Increase the amount of waste being recycled to 40%.			x	
Sustainability training and communications for employees.			x	
Partnership working with local groups and organisations to support sustainable development.			x	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			x	