NHS
Newcastle Gateshead
Clinical Commissioning Group

Standard Operating Procedure	CCG SOP15 Confidentiality Audit Procedure

Version	**2**
Implementation Date	**17/03/2016**
Review Date	**01/03/2018**
Approved By	**Executive Committee**
Approval Date	**15/03/2016**

Revisions

Date	Section	Reason for Change	Approved by
March 2016	All	Review and minor amendments	Executive Committee

Procedure Obsolete

Date	Reason	Approved by

1. Overview

This document establishes an approach to monitor access to the confidential information held by NHS Newcastle Gateshead CCG and provides assurance that the necessary controls are in place to manage access to confidential information. This work forms part of the CCG overall assurance framework and meets requirements within:

- The NHS Care Record Guarantee
- The Information Governance Toolkit
- The Confidentiality NHS Code of Practice

2. Introduction

With advances in the electronic management of health and employment information within the NHS the requirement to monitor access to confidential information has become increasingly important. Furthermore, with the increased use of electronic communications, the movement of confidential information via these methods poses an increasing threat of information falling into the hands of individuals who do not have a legitimate right of access to it. Organisations should therefore have processes to highlight actual or potential confidentiality breaches in their systems, particularly where person identifiable information is held.

The CCG has a responsibility to ensure that confidential information is protected. Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purposes may result in a breach of that confidentiality, therefore contravening the requirements of Caldicott, the Data Protection Act 1998 and the Common Law Duty of Confidentiality.

These procedures provide an assurance mechanism by which the effectiveness of controls implemented within the CCG are audited, areas for improvement and concern highlighted and recommendations for improved control and management of confidentiality within the organisation made.

3. Intended Audience

All CCG staff including temporary workers, locums and staff seconded or contracted from other organisations.

4. Responsibilities

Caldicott Guardian

The Caldicott Guardian will be responsible for monitoring incidents and complaints relating to confidentiality breaches within the CCG.

The Caldicott Guardian will be responsible for ensuring that access to personal information is regularly audited within the CCG.

They will be responsible for ensuring that concerns and recommendations arising from confidentiality audits are actioned within a reasonable timescale.

NECS ICT Service

The NECS ICT department will be responsible for ensuring that monitoring reports produced from computer systems are reviewed and followed up.

NECS IG Service / CCG IG Lead

The NECS IG department along with the CCG IG Lead will be responsible for ensuring the Confidentiality Audit procedure is implemented throughout the CCG and the monitoring of implementation. Audits and spot checks to be carried out at least annually with any concerns reported to the Caldicott Guardian.

Information Asset Owners (IAOs)

Information Asset Owners have the responsibility to provide assurance that information risk is being managed effectively in respect of the information assets they 'own'.

Information Asset Administrators

Information Asset Administrators have day to day responsibility for managing risks to one or more individual databases or systems.

All Staff

All staff are responsible for ensuring that they comply with local access monitoring procedures when requesting access to confidential records. All staff should ensure that confidential information is not accessed either personally or by other individuals without prior authorisation and establishment of a lawful basis. For further advice contact the NECS IG team.

All staff will be responsible for complying with confidentiality audits conducted within their area. They will be responsible for complying with recommendations which are made as a result of such audits.

5. Monitoring and Auditing Access to Confidential Information

5.1 Monitoring Access to Confidential Information

5.1.1 In order to provide assurance that access to confidential information is gained only by those individuals who have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis.

5.1.2 Monitoring should be carried out by IAA's and the NECS IG Team in order that irregularities regarding access to confidential information can be identified, reported to the IAO and Caldicott Guardian and action taken to

address the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

5.1.3 Actual or potential breaches of confidentiality should be reported to the CCG IG Lead and logged on the SIRMS system immediately in order that action can be taken to prevent further breaches taking place.

5.1.4 The Caldicott Guardian and NECS IG Team will be responsible for ensuring that the NHS Newcastle Gateshead CCG Executive Committee is informed of any concerns highlighted as a result of monitoring access to confidential information.

5.1.5 Should unauthorised access to confidential information be gained by any individual, this will be dealt with in accordance with the CCG procedures

5.2 Auditing Access to Confidential Information

5.2.1 The NECS IG Team will ensure that audits of security and access arrangements are conducted within the CCG on a regular basis. Areas to be audited should include:

- Security applied to manual files e.g. storage in locked cabinets / locked rooms
- Arrangements for recording access to manual files e.g. tracking cards, access requests by staff to their personnel files / interviewees to interview notes
- Permissions for access to electronic information, such as shared drives/databases
- Evidence that checks have been carried out to ensure that the person requesting access has a legitimate right to do so
- The use of disposal arrangements for post-it notes, notebooks and other temporary recording material
- Retention and disposal arrangements
- The location of answer phones which receive confidential information e.g. messages should be accessed where confidential information cannot be overheard
- Confidential information sent or received via email e.g. security applied and email system used
- Information removed from the workplace e.g. authorisation gained for short or long term removal
- Security arrangements applied e.g. transfer via secure methods. The understanding of staff within the CCG of their responsibilities with regard to confidentiality and restrictions on access to confidential information
- Security applied to laptops and compliance with the NECS Access Control Policy

5.3 Audit Method

5.3.1 The audit should be carried out through questionnaires and spot checks on at least an annual basis or more frequently if the need arises. Where issues and / or incidents are identified and informal interview would be carried out by the CCG IG Lead.

5.4 Frequency

5.4.1 Audits and spot checks to be carried out on a quarterly basis e.g. 5 questionnaires are distributed quarterly to staff and a spot check of one department to be carried out.

5.4.2 Each questionnaire will contain a unique reference number which will be used on all documentation collated and used within the exercise in order to determine in which quarter the audit was undertaken. (Appendix 1)

5.4.3 Once all questionnaires are completed and have been reviewed by the NECS IG Team the results will be passed to the CCG IG Lead. Any concerns should be appropriately addressed.

5.5 Choosing Appropriate Auditors

5.5.1 Audits should be conducted by appropriate individuals who have no connection with the work function being audited in order that an objective view can be achieved.

5.5.2 It is recommended that the individuals selected have a good knowledge of the requirements of the Data Protection Act 1998 and Caldicott Principles etc.

5.6 Audit Checklist

5.6.1 An audit checklist should be produced to enable the auditor to track progress of the audit. (Appendix 2)

5.7 Staff Awareness Interviews

5.7.1 Staff awareness interviews (if required) give the auditor an opportunity to assess the level of awareness of confidentiality issues. Interviews will be conducted, the duration of which will be 15 to 30 minutes.

5.7.2 The auditor's questions and the interviewees' responses should be recorded on the interview record sheet (Appendix 3) and not be restricted to only negative observations. This will enable the final report to show a balanced view.

5.8 Reporting

5.8.1 The outcome of the audit will provided to the CCG IG Lead and Caldicott Guardian as a formal report which will provide them with information as to CCG compliance with confidentiality requirements including functions and processes which comply and those which do not. The CCG IG Lead and Caldicott Guardian can then identify areas for improvement and assign actions to ensure that the CCG fulfils all requirements.

5.9 Non-Compliance / Concerns Observed

5.9.1 Where non-compliance is observed, this should be recorded as soon as possible, be sufficiently detailed, include all of the facts and refer to any relevant evidence (Appendix 4).

5.9.2 The detail should include what was observed, where it was observed, the date of the observation and why it was considered non-compliant.

5.9.3 Each instanced of non-compliance observed should have an associated recommendation recorded which should be discussed and agreed with the CCG IG Lead and Caldicott Guardian. The CCG IG Lead will ensure that the recommendation is implemented.

5.9.4 Where a number of instances of non-compliance are observed in the same department this may indicate a more serious problem within that area. If this is the case the CCG IG Lead and Caldicott Guardian will be informed, training needs identified and appropriate action taken.

5.9.5 There may be instances where the auditor is concerned by what has been observed but the instances are not non-compliances. The auditor will make recommendations for improvements to be made on the Confidentiality Audit Compliance Checklist (Appendix 4) in order that potential problems do not occur.

6. Audit Follow-Up

6.1 Any recommendations will be followed up by the CCG IG Lead and NECS IG Team to ensure that appropriate action has been taken.

Appendix I

Confidentiality Audit Questions

1. Where would you find the CCG IG policies and procedures?

a) Intranet
b) publication scheme
c) both

2. What is the principal NHS staff guide concerning patient confidentiality?

a) Code of Confidentiality
b) Faxing guidelines
c) FOI Act

3. How often must you complete mandatory IG refresher training?

a) every 2 years
b) every six months
c) annually

4. If you have direct contact with patients should you be explaining why you are collecting information about them and what you will do with it?

a) yes
b) no
c) don't know

5. What do you do if you are unable to answer a complex query about how NECS uses patient information?

a) refer to the relevant procedure
b) ask my line manager
c) refer to the NECS IG Team
d) a and c above

6. Who would you refer patients to concerning a request for access to records

a) reception
b) your Manager
c) the NECS IG Team

7. If you lose or find a smartcard you should

a) report this to the Registration Authority team immediately and report the incident
b) cut the card up and throw it away
c) keep it in your desk in case the owner comes looking for it.

8. Is it acceptable to share smartcards?

a) yes, it saves having to keep logging into the system
b) yes, you can still do your job if you forget or lose your card
c) no, smartcards must never be shared with anyone

9. Before sharing patient information, wherever possible, it should be:

a) anonymised,
b) encrypted
c) deleted

10. In accordance with the Information Lifecycle Management Procedure, documents should

a) be named
b) include version control
c) be securely stored
d) all the above

11. Any new information assets containing patient information should be:

a) declared to the responsible information asset owner
b) recorded in the information asset register
c) risk assessed to mitigate any information security issues
d) all of the above

12. If you discover a breach of confidence you should:

a) reprimand the offender
b) tell the patient
c) submit an incident form

13. Telephone messages containing patient information should be received by

a) secure voice mail
b) insecure answer phone
c) nearest passer by

14. Is it acceptable for staff to discuss patients where other people can hear?

a) Yes
b) No

15. What is a safe haven?

a) a special fax machine
b) a secure repository for patient information
c) a refuge for homeless people

16. You should never connect personal equipment into your laptop or PC Because:

a) risk of transferring viruses
b) the network will crash
c) a and b

17. The CCG Senior Information Risk Owner is:

a) Neil Morris
b) Joe Corrigan

Appendix 2

Confidentiality Audit Questionnaire Report

Year:	**Quarter 1**	**Quarter 2**	**Quarter 3**	**Quarter 4**
Question 1:	Where would you find the CCG IG policies and procedures?			
% correct				
Question 2:	What is the principle NHS staff guide concerning patient confidentiality?			
% correct				
Question 3:	How often must you complete mandatory IG refresher training?			
% correct				
Question 4:	If you have direct contact with patients should you be explaining why you are collecting information about them and what you will do with it?			
% correct				
Question 5:	What do you do if you are unable to answer a complex query about how NECS uses patient information?			
% correct				
Question 6:	Who would you refer patients to concerning a request for access to records:			
% correct				
Question 7:	If you lose or find a smartcard you should:			
% correct				
Question 8:	It is acceptable to share smartcards because:			
% correct				
Question 9:	Before sharing patient information, wherever possible, it should be:			
% correct				
Question 10:	In accordance with the Information Labelling and Classification Procedure, documents should include:			
% correct				
Question 11:	Any new information assets containing patient information should be:			
Question 12:	If you discover a breach of confidence you should:			

% correct				
Question 13:	Telephone messages containing patient information should be received by:			
% correct				
Question 14:	Is it acceptable for staff to discuss patients where other people can hear?			
% correct				
Question 15:	What is a safe haven:			
% correct				
Question 16:	You should never connect personal equipment into your laptop or PC because:			
% correct				
Question 17:	The CCG Senior Information Risk Owner is:			
% correct				

Appendix 3

Interview Record Sheet

Department/Area:	**Audit Date:**	**Audit Reference:**
Attendees:		
Name:	**Position:**	**Time in Organisation:**
DETAILS OF INTERVIEW		
Question 1	**[Enter question here]**	
Question 2	**[Enter question here]**	
Question 3	**[Enter question here]**	
Question 4	**[Enter question here]**	
Question 5	**[Enter question here]**	
Question 6	**[Enter question here]**	

Appendix 4

Confidentiality Audit Compliance Checklist

Compliance Check	Observations and Recommendations
PCs: Are users logged out / password screen saver activated when PC is left unattended	
Photocopiers / printers: Has all confidential information been removed	
Clear desk: Ensure that confidential information is not left on desks overnight / when staff leave the office	
USB sticks: Ensure USB sticks are encrypted	
Laptops: Ensure that laptops are locked away when not in use. Check laptops are encrypted.	
Confidential waste: Ensure confidential waste is appropriately destroyed e.g. placed in secure confidential waste bins	
Access to PID – paper files: Ensure confidential information is kept in locked drawers / cabinets when not in use	
Access to electronic information – ensure permissions are set correctly and reviewed regularly	
Access to areas: Check physical security mechanisms are working appropriately i.e. electronic door locks are in place	

Office Use Only	
Department:	**Date:**
Auditors Name:	**Auditors signature:**