CONFIDENTIALITY AUDIT PROCEDURE:

Document History

Document Reference:	IG15
Version:	Revised Policy
Ratified by:	SL/SWL CCG Senior Leadership Teams
Date ratified	March 2018
Name of originator/author	Information Governance Services
Name of responsible committee/individual:	Senior Leadership Team
Date issued:	March 2018
Review Date:	February 2021
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Website
Document Purpose:	This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations' information is maintained.

South Lincolnshire CCG
South West Lincolnshire CCG

Version control sheet

Version	Section/Para/Appendix	Version/Description of Amendments	Date	Author/	Version
Revised Version Serving SL and SWL CCGs (dual branding)	Policy Review	Incorporates specific reference to impending General Data Protection Regulation (Revised as a dual branded policy for NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG) Replaces existing policies within SL and SWL CCG referenced IG15.	27/02/2018	JE	1

ASSISTANCE WITH THE APPLICATION OF THIS POLICY AND UPDATES

This policy has been prepared so as to reflect the law as at 14 February 2018. The policy will require periodic review to reflect subsequent changes to the law. Under the General Data Protection Regulation (GDPR) (which will apply from 28th May 2018), personal data must be processed in accordance with certain principles. While these are broadly similar to those under the Data Protection Directive (DPD), the wording has changed and they all centre around the concept of accountability.

The GDPR applies to 'controllers' and 'processors'; A controller determines the purposes and means of processing personal data whilst a processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR applies to those who have a day to day responsibility for data protection. This should be read in conjunction with the CCGs' Information Governance Staff Handbook.

CONTENTS

CONFIDENTIALITY AUDIT PROCEDURE

1 Background

1.1 All Clinical Commissioning Groups (CCGs) should already have control mechanisms in place to manage and safeguard confidentiality, including mechanisms for highlighting problems such as incidents, complaints and alerts. This further requirement asks that documented procedures are implemented to ensure these controls are monitored and audited and is part of the key assurance requirement of the information governance toolkit.

1.2 Organisations should have processes to highlight actual or potential confidentiality breaches in their systems, particularly where personal confidential data (PCD) is held. They should also have procedures in place to evaluate the effectiveness of the controls within the systems.

1.3 Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented may result in a breach of that confidentiality, therefore contravening the requirements of the Caldicott Report, the Data Protection Act, the Human Rights Act and the Common Law duty of Confidentiality.

2 Purpose

2.1 This document sets out the procedure for carrying out audits relating to access to personal confidential information for the CCG.

2.2 The purpose of this procedure is to ensure that staff only access information where there is a legitimate business need and to meet the requirement of the Information Governance Toolkit.

3 Scope

3.1 This procedure applies to all staff who work for or on behalf of the CCG including those on a temporary basis, seconded, volunteers and students.

3.2 All work areas within the CCG which process personal confidential information will be subject to the confidentiality audit procedures.

4 Responsibilities and Accountabilities

4.1 The organisation should ensure that overall responsibility for monitoring and auditing access to confidential information is allocated to an appropriate senior staff member or equivalent. The Senior Information Risk Owner (SIRO) and Caldicott Guardian will be updated with the findings of any confidentiality audits and ensure that appropriate action is taken.

4.2 The IG Team at Optum Commissioning Support Services will ensure that the confidentiality audit procedure is reviewed and updated in line with

national requirements and support the CCG with investigations and onward reporting to the SIRO or Caldicott Guardian. For further information contact lynne.wray1@nhs.net or jemptage@nhs.net

4.3 The SIRO 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 the SIRO is responsible for.

4.4 Monitoring should be carried out by the SIRO supported by the Information Governance (IG) lead at GEMCSU. The findings should be reported to the SIRO and Caldicott Guardian and action taken where necessary regarding the implementation of any controls or remedial action to address the situation.

4.5 Line managers should ensure that all new starters complete the appropriate information governance training on commencement and prior to accessing any confidential information. They must also ensure that staffs are aware of the mechanisms for reporting potential or actual breaches of confidentiality and the consequences regarding disciplinary processes.

4.6 Across the Lincolnshire Clinical Commissioning Groups (CCGs) incident reports and any potential breaches of confidentiality or security will be reported through the SIRO/Caldicott Guardian or CCG leads to the CCG IG Working Group.

5 Process

5.1 Confidentiality audits will focus primarily on controls within electronic information management systems, but should not exclude paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of the system, or as a result of weak, non-existent or poorly applied controls.

5.2 The audit will look for staff awareness of CCG confidentiality and security processes; appropriate use of faxes and hard copy personal confidential information; security of email processes and physical security of work areas.

5.3 The following are examples of events that the organisation should audit for frequency, circumstances, location etc:-

- Failed attempts to access confidential information
- Repeated attempts to access confidential information
- Successful access of confidential information
- Evidence of shared logons

5.4 Audits will be carried out in one of two ways:

a) Through a regular audit programme where a department or areas of the organisation has been identified for a confidentiality audit. in response to a request from a particular team or department, either through raised concerns regarding confidentiality processes

5.5 In response to concerns regarding confidentiality processes from a particular team or

department. As part of a CCG initiated programme of audits Confidentiality Audit procedures should be communicated to all staff with the potential to access personal confidential information. The organisation has a responsibility for providing appropriate training and support to ensure the individual can carry out their role. Disciplinary procedures should outline the penalties for unauthorised access or attempts, eg suspension or bringing criminal charges.

5.6 As part of the process of shared learning, the results of audits may be presented to the Information Governance Committee (or equivalent) on agreement of the participating CCG.

6 Investigating Confidentiality Events

6.1 Where non-compliance is observed, this will be recorded as soon as possible. Where there are recommendations, this should be discussed with the team member and other staff as appropriate and a target date for completion of any remedial action.

6.2 If it is considered that a breach of confidentiality has occurred, then the procedure for investigation of security breaches (see the CCGs organisations Incident Reporting Procedure) will be followed.

6.3 Unauthorised access to confidential information by any individual will be considered against the CCGs disciplinary procedures.

7 Summary Care Record

7.1 Summary Care Record (SCR) has been designed to ensure that Information Governance (IG) safeguards are in place to enable staff to access summary information about a patient when it is relevant to their job and appropriate to do so. SCR uses the following IG controls to ensure that Care Record Guarantee rules are adhered to:

- Authentication and Role Based Access Controls (RBAC)
- Legitimate relationships
- Permission to view

7.2 Access to national applications (such as the SCR) will be set up by the data controller of the system (for example the general practice) and it will be the responsibility of the practice to ensure that the access given to external staff or partners is appropriate and role-based. The role of the Privacy Officer is to receive and monitor any alerts generated.

8 Equality and Diversity

8.1 This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marital status or civil partnership. The CCG aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a

disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

8.2 This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

8.3 In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

9 Review of the Procedure

9.1 This procedure will be reviewed by the CCG IG Working Group annually. This may be subject to change and the policy may be reviewed in the event of serious untoward incidents or a change in national guidance.

10 References

NHS Code of Confidentiality

11. APPENDIX A – AUDIT QUESTIONNAIRE

It will assist the audit process for the area to be audited to complete the pre-audit questionnaire. This will enable the auditor to gain an understanding of the function of the department and the processes carried out relating to confidential information.

The auditor will then arrange a pre-audit meeting with key personnel to discuss the process.

Information Security and Confidentiality Audit

Service/Team:	
Location / Base*:	
Department:	
Service Team Manager / Team Leader:	
Date of Audit:	
Contact No:	

Instructions for use

Service Managers must complete both Part 1 and Part 2 of the attached questionnaire.

**If the service is based in different locations. (A separate audit must be conducted for each base.)*

Part 1 includes information about the Service/Team's Information Security and Confidentiality Practices and Procedures.

Part 2 contains questions regarding individual staff knowledge regarding Information Security and Confidentiality knowledge.

If using this form electronically, tab through the shaded boxes. Press the Spacebar to enter an X in the box or for 'free text' boxes, type as usual.

Save the document with your service team name and e-mail to the address below.

Please complete both parts and return to:

Information Governance Team
South Kesteven District Council Offices
c/o Optum CSS Offices – Suite 2
St. Peter's Hill,
Grantham
Lincolnshire
NG31 6PZ
E-mail: jemptage@nhs.net

Please complete the questions as follows:

Does your service/team have documented procedures which include local security and confidentiality procedures?	**Yes** ☐ **No** ☐	
Are your internal offices lockable?	**Yes** ☐ **No** ☐	Go to Q3 Go to Q4
Do you have access codes for doors?	**Yes** ☐ **No** ☐	Go to Q3a Go to Q4
How often are these changed? *(i.e. 6 months)*	**Every**	**Months**
Do you have security procedures for visitors:	**Yes** ☐ **No** ☐	Go to Q4a Go to Q5
These are: (*Please mark each as appropriate)* Visitors Book Reporting to Reception Visitor is collected Other *(Please state below)*	☐ ☐ ☐ ☐	
Do you store any paper based information which contains patient identifiable information?	**Yes** ☐ **No** ☐	Go to Q5a Go to Q6
If yes, how do you ensure its security: • Office premises locked out of hours • Confidential files stored in a locked filing cabinet, cupboard, or similar • Other: *(please state)*	***Tick as appropriate*** ☐ ☐ ☐	
Is electronic personal confidential information (on the computer information stored on the C:Drive, Shared Network Drive *(such as the G: Drive, H:Drive)* or both? *NB: This does not include information stored on SystmOne or clinical systems*	**C:Drive** ☐ **Network** ☐ **Both** ☐	Go to Q6a Go to Q7 Go to Q6a
If information is stored on the C:Drive, please state the reason: *(i.e. no access to network facilities, working remotely):* • Provide details of back up procedures: • Provide details of storage for back up disks.		

7	If personal confidential information is stored on the Shared Network Drive *(such as the G: Drive, H:Drive),* how do you ensure its security: • Folders/directories on network are limited so that only authorised persons can access files in them? • Portable computers are secured with a password? • No Patient Identifiable information is stored on the C:Drive? • Other: *(please state)*	***Tick as appropriate*** ☐ ☐ ☐ ☐	
8	Do all computers within the Service/Team have password protected screensavers?	**Yes** ☐ **No** ☐	
9	Is personal confidential information ever taken out of the base:	**Yes** ☐ **No** ☐	Go to Q9a Go to Q10
9a	If so, state the reason for this: • Working from home • Working at other locations/bases • Other: *(please state)*	***Tick as appropriate*** ☐ ☐ ☐	
9b	How do staff members ensure the security of information outside of the base? *(Please state)*		
10	Does your base follow clear desk guidelines? *(i.e. files are locked up at the end of the day)*	**Yes** ☐ **No** ☐	
11	Does your Service/Team disclose personal confidential information outside of the organisations *(including independent contractors such as dentists, GPs etc)*?	**Yes** ☐ **No** ☐	Go to Q11a Go to Q12
11a	Have staff members been made aware of the Information Governance staff briefing and where this can be found?	**Yes** ☐ **No** ☐	
12	Do staff members have access to the information governance resources on the intranet?	**Yes** ☐ **No** ☐	

13	Do staff members within the Service/Team have private offices, where telephone calls can be made without being overheard by anyone else?	**Yes** ☐ Go to Q14 **No** ☐ Go to Q13a
13a	If no, please state who is located in the same office: • Other members of the Service/Team? • Other members of other teams? • Patients/clients • Occasionally, other visitors	***Tick as appropriate*** ☐ ☐ ☐ ☐
13b	Is there a private office staff can use if they require complete privacy?	**Yes** ☐ **No** ☐
14	Can any unauthorised people access your Service/Team's incoming mail?	**Yes** ☐ **No** ☐
15	Before you or a member of your staff collects your mail, is it stored in a secure place?	**Yes** ☐ **No** ☐
16	Does your Service/team send and/or receive personal Identifiable information via fax	**Yes** ☐ Go to 17 **No** ☐ Go to part 2
17	Please confirm your fax machine number	
18	Please confirm where the fax machine is situated • Reception • Office • Other (please state)	***Tick as appropriate*** ☐ ☐ ☐
19	Can you confirm briefly what information is faxed	

Confirm where you send fax information to?	***Tick as appropriate***
General Practice	☐
Other CCGs	☐
Acute Trust (Sherwood Forest e.g. Hospital)	☐
Local Authority	☐
Other NHS Organisations – *(please state)*	☐
Other external Organisations – *(please state)*	☐

Confirm where you receive faxes information from?	***Tick as appropriate***
General Practice	☐
Other CCGs	☐
Acute Trusts – eg Sherwood Forest Hospital	☐
Local Authority	☐
Other NHS Organisations – *(please state)*	☐
	☐
Social Care	
Other External Organisations – *(please state)*	

Is the fax machine a secure area which can only be accessed by your Service/Team staff	**Yes**	☐
	No	☐
Do you confirm contact recipient if they have received the sent fax (safe haven)	**Yes**	☐
	No	☐
Do you use removable media (eg memory sticks and other storage devices)	**Yes**	☐
	No	☐

If you use removable media, is this encrypted?	Use	Encrypted
Data stick	☐	☐
CD/DVD	☐	☐
Camera	☐	☐
Smartphone	☐	☐
Other – Please specify	☐	☐
If responded NO, complete question 26		

Where removable devices do not have encryption, please detail any measure in place to keep the data secure?

27	Do you email any personal confidential data? (including NHS number only) ***If responded NO, complete question 31***	**Yes** **No** ☐ ☐
28	Can you confirm the type of information that is emailed?	
29	Do you use NHS mail to send PCD?	**Yes** **No**
30	Do you Use safe haven principles when sending emails? *(ie check the correct recipient before sending)*	**Yes** **No** ☐ ☐
31	Can you please confirm if you send/receive any data from outside the UK	**Yes** **No** ☐ ☐
30a	If so from which countries, please list	☐ ☐

Comments Regarding this Audit

We welcome your feedback to ensure that this audit form is easy to use and understand.

If you have any comments regarding the content, understanding and ease of use of the form, please include these below.

If you have any questions or comments about any specific questions, please indicate the question number next to the comment.

Comments.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Confidentiality Audit Procedure

Brief description of the proposal:

To ensure that the policy amends are fit for purpose, that the policy is legally compliant, complies with legislative requirements and includes details of the European Directive – General Data Protection Regulations.

Name(s) and role(s) of staff completing this assessment:

June Emptage – Information Governance Officer

Date of assessment: 27 February 2018

proposed change:

Will it affect employees, customers, and/or the public? Please

state which.

Yes it will affect all employees and those who enter into contractual arrangements with the organisation.

Is it a major change affecting how a service or policy is delivered or accessed?

No – although it introduces new General Data Protection Regulations which will be mandatory in May 2018

Will it have an effect on how other organisations operate in terms of equality?

No

If you conclude that there will not be a detrimental impact on any equality group, caused by the proposed change, please state how you have reached that conclusion:

No anticipated detrimental impact on any equality group. The policy adheres to the legislative requirements which are applicable to all.