



CALDICOTT FUNCTION PLAN:

Document History

Document Reference:	IG19
Version:	Revised Policy
Ratified by:	SLCCG /SWLCCG 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 IG19.	26/02/2018	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 on 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 and the Privacy Impact Assessment Policy.

CONTENTS

Section		Page
1	Introduction & Aims	3
2	Scope	3
3	The Confidentiality and Data Protection Work Programme detailing Caldicott Guardian Responsibilities (IGT Requirement 14_1-230 1a)	3
4	Training	5
5	The Caldicott Function	5
6	Accountability	5
7	Equality and Diversity	6
8	Due Regard	6
9	Review	6
	Appendix 1 – Equality Analysis Initial Assessment	7

1. Introduction and aims

1.1 The purpose of this document is to provide guidance to NHS South Lincolnshire and NHS South West Lincolnshire Clinical Commissioning Group (CCG) staff on the CCG's Caldicott Function Plan.

1.2 The aims of this document are to ensure that:

- Individuals are aware of the CCG's mandatory responsibilities in relation to confidentiality issues and their own.

2. Scope

2.1 This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. This policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

3. The Confidentiality and Data Protection Work Programme detailing Caldicott Guardian Responsibilities (IGT Requirement 14-230 1a)

3.1 The recommendations of the Caldicott Committee (1997 Caldicott Report) defined the confidentiality agenda for National Health Service (NHS) organisations. A key recommendation was the appointment in each NHS Trust and special health authority (e.g. NHS Business Services Authority) of a 'Guardian' of patient identifiable information to oversee the arrangements for the use and sharing of patient information. Guardians were mandated for the NHS in Health Service Circular 1999/012 and were introduced into social care in 2002, mandated by Local Authority Circular LAC 2002/2).

3.2 Strategy & Governance: the Caldicott Guardian should champion confidentiality issues at Board/senior management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

3.3 Confidentiality & Data Protection expertise: the Caldicott Guardian should develop knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available. Optum Commissioning Support Services (Lynne.wray1@nhs.net or jemptage@nhs.net) provides this functionality on behalf of the CCG.

3.4 Internal Information Processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

3.5 Information Sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared

with external bodies both within, and outside, the NHS and Councils with Social Care Responsibilities (CSSRs). This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related new IT systems, disclosure to research interests and disclosure to the police.

4. Training

4.1 The Role of the Caldicott Handbook must be completed on an annual basis and a copy is available here:

<https://www.igt.hscic.gov.uk/NewsArticle.aspx?artid=170>

5. The Caldicott Function

5.1 The key responsibilities of the Caldicott Function are to:

- Support the Caldicott Guardian
- Ensure the confidentiality and data protection work programme is successfully coordinated and implemented
- Ensure compliance with the principles contained within the confidentiality: NHS code of practice and that staff are made aware of individual responsibilities through policy, procedure and training;
- complete the Confidentiality and Data Protection Assurance component of the Information Governance Toolkit, contributing to the annual assessment;
- provide routine reports to the senior management on Confidentiality and Data Protection issues;
- identify and address any barriers for sharing for care

5.2 The Caldicott Guardian Manual sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as a part of broader information governance. Further information relating to the UK Caldicott Guardian Council (UKCGC) – the national body for Caldicott Guardians is available

<https://www.gov.uk/government/groups/uk-caldicott-guardian-council>

On this site, the following information is available:

- details regarding the Aims of the Council
- Manual for Caldicott Guardians
- Caldicott Guardian Registration details
- Contact details

6. Accountability

6.1 Overall responsibility for the Caldicott Function Plan sits with the Chief Officer who has delegated responsibility for managing the development and implementation of procedural documents to the Caldicott Guardian in the CCG. Support is provided from OPTUM Commissioning Support Services (Information Governance Team) under contract. The CCG may take disciplinary action against users found to have contravened this Plan.

6.2 Access and the removal of users' access to CCG systems hosted by the Commissioning Support Service, can only be started after proper investigation procedures are completed.

7. Equality and Diversity

- 7.1 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.
- 7.2 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.
- 7.3 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.

8. Due Regard

- 8.1 This policy has due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations

9. Review

- 9.1 This plan will be reviewed annually in line with Information Governance Toolkit requirements or where changes occur with legislation or national policy.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Caldicott Function Plan

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: 15 February 2018

Please answer the following questions in relation to the 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.