Confidentiality and Data Protection Policy

Document History

Document Reference:	IG03
Version:	Revised Policy
Ratified by:	SLCCG /SWLCCG SENIOR LEADERSHIP TEAMS
Date ratified	March 2018
Name of originator/author	Information Governance Services, OPTUM CSS
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 Confidentiality and Data Protection Policy aims to detail how the CCG meets its legal obligations and NHS requirements concerning confidentiality and information security standards.

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 IG03.	14/02/2018	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; The Privacy Impact Assessment Policy and the Records Management Policy.

CONTENTS

1. QUICK REFERENCE GUIDE

1.1 The CCG has a legal duty to comply with the Data Protection Act 2018 and with effect from 25th May 2018, the General Data Protection Regulations.

1.2 All staff members are responsible for maintaining compliance with the Data Protection Principles and for reporting non-compliance, or where a near miss has occurred, through the CCG's incident reporting process via Datix.

1.3 Under a provision of the Data Protection Act an individual can request access to their personal information regardless of the media in which this information may be held / retained. The CCG has a Subject Access Procedure for dealing with such requests. In the first instance, individuals wishing to exercise their right of access should make a written application to the CCG holding the records, including via email.

1.4 There is a requirement to make the general public, who use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed.

1.5 Patients must be made aware of this requirement by the use of information leaflets, posters, statements in patient handbooks and verbally by those healthcare professionals providing care and treatment. The CCG is obliged to produce patient information leaflets and posters explaining the uses of patient information.

1.6 Point 5 is particularly important as a CCG is not legally entitled to send or receive Personal Confidential Data (PCD) unless explicit consent has been obtained from the patient to process their information OR 2) another statutory gateway applies.

1.7 Staff contracts of employment are produced and monitored by the CCG Human Resources Department. All contracts of employment include Information Governance clauses, including information governance and data protection responsibilities.

1.8 A breach of the Data Protection requirements could result in a member of staff facing disciplinary action. All staff must adhere to CCG policies and procedures relating to the processing of personal information.

1.9 There are Acts of Parliament that govern the disclosure / sharing of PCD. Some make it a legal requirement to disclose whilst others state when information cannot be disclosed. The Health and Social Care Information Centre (HSCIC) Guide to Confidentiality 2013 gives clear guidance on disclosure of patient information.

1.10 Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, the public rightly expects that their personal data will be properly protected. Information sharing protocols provide the basis for facilitating the exchange of information between organisations.

1.11 It is a CCG requirement that patients are told how their information is to be used before they are asked to provide it or as soon as is possible. Specific information must be given to patients about the use of their personal information, particularly if for uses other than the provision of healthcare. The explicit consent of the patient must be obtained before information is processed for reasons other than the direct provision of healthcare e.g. used for research purposes, invoice validation.

1.12 The use of Privacy Impact Assessments is required to help the CCG to comply with

Privacy by Design principles and should be considered for all new projects and proposals affecting the management of personal data.

1.13 All staff members are required to assess the likelihood of a risk to the confidentiality and security of personal information during transfer and on receipt and adopt Safe Haven Principles to ensure person confidential data can be held, received and communicated securely.

1.14 Information Asset Owners (or equivalent) are required to ensure there is a documented policy for approvals and authorisation for mobile working and teleworking arrangements, and undertake information security risk assessments for each of the CCG's Information Assets taking into consideration the potential impacts to the protection of personal and corporate data. All staff members are required to be mindful of upholding public confidence in the CCG's ability to ensure the confidentiality and integrity of person confidential data.

1.15 All staff members are required to ensure that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements.

1.16 All staff members are responsible for the security and confidentiality of personal/corporate, sensitive/corporate sensitive information they process.

1.17 All staff with the potential to access confidential personal information/ sensitive/corporate/corporate sensitive information to be aware that access to confidential personal information is monitored and audited locally.

1.18 All staff members are responsible to ensure that personal/corporate records are accurate and kept safely and confidentially and respect confidentiality when personal information is held in confidence.

2. INTRODUCTION

2.1 The CCG has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by NHS England and the Information Governance Alliance, the Information Commissioner (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

2.2 All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the CCG. Penalties could be imposed upon the CCG and/or CCG employees for non-compliance with relevant legislation and NHS guidance.

3. PURPOSE

3.1 This Data Protection Policy aims to detail how the CCG meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are primarily based upon the key piece of legislation, the Data Protection Act 1998, however, other relevant legislation and appropriate guidance will be referenced. The General Data Protection Regulations (GDPR) will become law on 25th May 2018.

4. SCOPE

4.1 This Policy applies to all staff within NHS South Lincolnshire and South West Lincolnshire Clinical Commissioning Groups (CCGs) and other personnel working for and on behalf of NHS South Lincolnshire and South West Lincolnshire Clinical Commissioning Groups including agency staff and contractors, to ensure that the CCG meets its legal requirements under the Data Protection Act 1998.

5. DEFINITIONS within the Data Protection Act 1998

5.1 **Data Controller:**
The person or organisation NHS South Lincolnshire and South West Lincolnshire Clinical Commissioning Group (CCG) that collects personal data and decides on how to use, store or distribute that data

5.2 **Data Processor:**
Any person or organisation (other than an employee of the data controller) that processes personal data on behalf of the data controller

5.3 **Data Subject:**
An individual who is the subject of the personal data

5.4 **Personal Data:**
Data that relates to a living individual that can identify the individual from this data or other information in the possession of the data controller

5.5 **Sensitive Personal Data:**
Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions

5.6 **Right of Subject Access:**
'Data Subjects' have the right to access and be given details of any information held about them that:

5.6.1 consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual for CCG staff, this includes the Personnel and Occupational Health record

5.6.2 where data has been obtained from the Health & Social Care Information Centre (HSCIC) via a Data Service for Commissioners Regional Office (DSCRO) advice must be sought from them prior to release to ensure compliance with the terms of any Data Sharing Contract that may be in force.

6 DUTIES AND RESPONSIBILITIES

6.1 The CCG has a legal duty to comply with the Data Protection Act 1998.

6.2 The Accountable Officer is responsible for ensuring that the responsibility for data protection is allocated appropriately within the CCG and that the role is supported; and is responsible for the implementation of this policy and for ensuring that:

6.2.1 All staff dealing with personal information are aware of the need for compliance with the Act and associated provisions

6.2.2 All staff are also aware of the requirements of the common law duty of confidence as set out in the HSCIC Guide to Confidentiality

6.2.3 The CCG is aware of the detailed provisions of the Act and secondary legislation and of any subsequent guidance issued by the Department of Health and by the Information Commissioner

6.2.4 The processing of personal data within the CCG is in compliance with the Act

6.2.5 Notification to the Information Commissioner (where required) of processing of personal data by the CCG is up to date

6.2.6 There is scheduled review of this policy

6.3 Information Asset Owners are responsible for understanding and addressing information governance risks relevant to the "information assets" that they own.

6.4 Managers and Information Asset Owners within the CCG are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

6.5 All staff must adhere to CCG policies and procedures relating to the processing of personal information.

6.6 All staff members are responsible for maintaining compliance with the Data Protection Principles and for reporting non-compliance through the CCG incident reporting process.

7. PROCESS

7.1 The legislation listed below also refers to issues of security and confidentiality of personal data:

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Data Protection Act 2018
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- The General Data Protection Regulations (GDPR)

7.2 **NHS and related guidance -** The following are the main publications referring to security and confidentiality of personal identifiable information:

- HSCIC : Guide to Confidentiality 2013Employee Code of Practice (Information Commissioner)
- Records Management Code of Practice for Health and Social Care 2016
- ISO/IEC 27001:2005 and 17799:2005 Information Security Standard
- Data Protection Act 1998 available from www.**opsi**.gov.uk
- Freedom of Information available from www.**opsi**.gov.uk
- Codes of Practice published by the Information Governance Alliance available via: https://digital.nhs.uk/codes-of-practice-handling-information
    - Records Management Code of Practice for Health and Social Care 2016
    - Code of Practice on confidential information
    - HSCIC Guide to Confidentiality 2013
    - Confidentiality: NHS Code of Practice

- Information Security Management NHS Code of Practice
- NHS Information Governance – Guidance on Legal and Professional Obligations
- General Data Protection Regulations - guidance – the 12 Steps

7.3 **Overview of the Data Protection Act 2018** - This Act applies to all person identifiable information held in manual files, computer databases, videos and other automated media, about living individuals. The Act dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff may result in disciplinary action.

7.4 **Information Sharing**

Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, the public rightly expect that their personal data will be properly protected. When sharing personal information, CCG staff must ensure that the Principles of the DPA 1998, the Human Rights Act 1998, the Caldicott Principles (including Caldicott 2) and the Common Law Duty of Confidentiality are upheld. Information sharing protocols provide the basis for facilitating the exchange of information between organisations.

7.5 **Data Protection Impact Assessments**

Data Protection Impact Assessments (PIAs) are a mandated requirement under the Data Protection Act 2018. DPIAs are intended to build in "privacy by design" and are also intended to prevent privacy related problems from arising, by: (i) Considering the impact on privacy at the project start (ii) Identifying ways of minimising any adverse impact and (iii) Building this into the project as it develops. The need for Data Protection Impact Assessments will be captured through the formal Business Case process and must be considered where any project or proposal will:

- Introduce a new or additional piece of IT that will relate to the management of PCD
- Introduce a new process that requires the use of PCD where it had previously been conducted anonymously
- Involve a change in how the CCG will handle either (a) large amounts of PCD about an individual, or (b) PID about a large number of individual

7.6 **Determining personal information**

The following flow chart can be used by staff to help assess when certain kinds of data may or may not constitutes Personal Data. Appendix 1 refers.

7.7 **Advice and Guidance -** Please contact the Information Governance Lead or OPTUM CSS for further advice relating to any form of disclosure of personal information e.g. disclosure to the police, the media etc. For advice and assistance in relation to the application of this policy and to obtain updates please contact: your line manager in the first instance or Optum Commissioning Support Unit, Council Offices, St Peters Hill, Grantham, NG31 6PZ e-mail jemptage@nhs.net

8. EQUALITY ASSESSMENT

8.1 Refer to Appendix 1 for a detailed description of the equality assessment undertaken for this policy.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Confidentiality Data Protection Policy

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: 14 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.