Derby and Derbyshire
Clinical Commissioning Group

Confidentiality and Data Protection Policy

Document History

Document Reference:	IG16
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
Date Approved:	12th September 2018
Approving Committee:	Information Governance Committee
Version Number:	1.0
Status:	
Next Revision Due:	September 2019
Developed by:	Information Governance Team
Policy Sponsor:	Derby and Derbyshire CCG Governance Committee
Target Audience:	All Staff within Derby and Derbyshire CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement, and to members , contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Associated Documents:	All Information Governance Policies and the Data Security and Protection Toolkit

Revision History

Version	Revision date	Summary of Changes
1.0	August 2013	Updated in line with NHS England, the Caldicott Review and version 11 of the Information Governance Toolkit
2.0	August 2014	Updated in line with version 12 Information Governance Toolkit
2.1	October 2014	Amended following feedback from CCGs.
2.2	June 2015	Updated in line with version 13 Information Governance Toolkit. References to GEM CSU updated to Arden & GEM CSU, web links and references updated.
2.3	July 2015	Update in line with CCG IG Leads comments
2.4	June 2016	Annual review and update
2.5	November 2017	Annual review and update
3.0	November 2017	Final – approved at IGC
3.1	June 2018	Reviewed to comply with the General Data Protection Regulation and the Data Protection Act 2018
3.2	September 2018	Final – approved at IGC

Policy Dissemination information

Reference Number	Title	Available from
IG16	Confidentiality and Data Protection Policy	Shared Drive

Contents

QUICK REFERENCE GUIDE 3
1. INTRODUCTION....6
2. PURPOSE 6
3. SCOPE 6
4. DEFINITIONS 6
5. DUTIES AND RESPONSIBILITIES....8
6. PROCESS 9
6.1 Selected Legislation....9
6.2 NHS and related guidance....10
6.3 Data Protection Principles....11
6.4 Individual Rights....12
6.5 Determining Personal Data....12
6.7 Caldicott Report Overview....14
6.8 Staff Issues....14
6.9 Disclosure of personal identifiable information....14
6.10 Keeping patients informed....15
6.11 Data Protection contractual clauses....15
6.12 Data Protection Impact Assessments....16
7 TRAINING REQUIREMENTS 16
8 EQUALITY AND DIVERSITY 17
9 DUE REGARD 17
10 REFERENCES AND ASSOCIATED DOCUMENTATION 17
11 MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF, PROCEDURAL DOCUMENTS 19
12 APPENDICES....20
Appendix A: Overview of legislation....20
Appendix B: Overview of NHS Guidance....22

QUICK REFERENCE GUIDE

1. The CCG has a legal duty to comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2. All staff members including third party contractors, volunteers and secondees 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.

3. Under a provision of the General Data Protection Regulation an individual can request access to their personal information regardless of the media in which this information may be held / retained. The CCG has got 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. A request can also be submitted via email.

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. This is facilitated through the CCG's Privacy Notice being available on the publically accessible Website with links to the relevant departments processing data.

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.

6. The CCG must meet the requirements of the Common Law Duty of Confidentiality (CLDC) to enable the processing of personal confidential data. Those requirements are-

   • A mandatory legal requirement or power that enables the CLDC to be set aside, such as The Children Act 1989 which requires information to be shared in safeguarding cases;

   • A court order where a judge has ordered that specific and relevant information is provided, and to whom;

   • An overriding public interest where it is judged that the benefit of providing the information outweighs the rights to privacy for the patient concerned and the public good of maintaining trust in the confidentiality of the service;

   • Explicit or implied consent; **OR**

   • Legal support for the use of the data without consent under the Health Services (Control of Patient Information) Regulations 2002, under section 251 of the NHS Act 2006.

   Consent

   There are two types of consent under the CLDC, which differ from the consent described in the DPA.

   • **Implied consent** will normally apply where data is being used to support individual care and treatment. For example, when a clinician refers a patient to another clinician

and this is explained to the patient, or when the patient has a reasonable expectation that data about them will be used in this way.

This type of consent will not usually be applicable to the purposes for which the CCG is processing personal data.

• **Explicit consent** applies where a patient has agreed to the use of data for a specified purpose, after they have been fully informed. Consent under CLDC does not need to meet the requirements for consent set out in the DPA.

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

8. A breach of the Data Protection requirements could result in a member of staff facing disciplinary action in line with the CCG's Disciplinary Policy. All staff must adhere to CCG policies and procedures relating to the processing of personal information.

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. NHS Digital (formerly HSCIC) Guide to Confidentiality: 2013 gives clear guidance on disclosure of patient information.

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.

11. The use of Data Protection Impact Assessments is required to help the CCG comply with Privacy by Design principles and is mandatory for all new projects and proposals affecting the management of personal data.

12. 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.

13. Information Asset Owners 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 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.

14. 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.

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

16. 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.

17. All staff members are responsible for ensuring that personal/corporate records are accurate and kept safely and confidentially and confidentiality is respected when personal information is held in confidence.

1. INTRODUCTION

This policy applies to Derby and Derbyshire CCG subsequently referred to as the CCG.

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 the Department of Health (DH), the Information Commissioner (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

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.

2. PURPOSE

This Confidentiality & 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 pieces of legislation, General Data Protection Regulation 2016 and the Data Protection Act 2018, however, other relevant legislation and appropriate guidance will be referenced.

3. SCOPE

This Policy applies to all staff within the CCG and other personnel working for and on behalf of the CCG including agency staff and contractors, to ensure that the CCG meets its legal requirements under the Data Protection Act 2018 and the General Data Protection Regulation.

4. DEFINITIONS

Consent – as defined under GDPR:

‘any freely-given specific and informed indication of [the data subject’s] wishes by which the data
subject signifies his agreement to personal data relating to him being processed’.

Data Controller:

The person or the organisation that collects personal data and decides on how to use, store or distribute that data

Data Processor:

Any person or organisation (other than an employee of the data controller) that processes personal data on behalf of the data controller

Data Subject or Natural Person:

An individual who is the subject of the personal data

Personal Data:

Data that relates to a living individual that can identify the individual from this data or from those data and other information which is in the possession of or is likely to come into the possession of the data controller

Special Category Data:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

Right of Subject Access:

‘Data Subjects’ have the right to access and be given details of any information held about them that:

- 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

They have the right to obtain the following:

•confirmation that the CCG is processing their personal data;

•a copy of their personal data; and

•other supplementary information – such as information in the 'Privacy Notice'

Some information may be withheld in line with the exemptions set out in the DPA such as:

- The information relates to a Third Party who has not consented to the disclosure
- The information could cause serious damage or harm to the mental / physical health of the person or any other person.

Where data has been obtained from NHS Digital 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 / Agreement that may be in force.

5. DUTIES AND RESPONSIBILITIES

The CCG has a legal duty to comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The requirements of the Common Law Duty of Confidentiality must also be met.

The Chief Executive / Accountable Officer through the Data Protection Officer is responsible for ensuring that the responsibility for data protection is allocated appropriately within the CCG and that the roles are supported.

The CCG is responsible for the implementation of this policy and for ensuring that:

- There is a Data Protection Officer appointed and details of the person holding that position along with contact information is publicised to staff and the general public
- All staff dealing with personal information are aware of the need for compliance with the Regulation/Act and associated provisions

- All staff are also aware of the requirements of the common law duty of Confidentiality as set out in the HSCIC Guide to Confidentiality
- The CCG is aware of the detailed provisions of the Regulation/Act and secondary legislation and of any subsequent guidance issued by the Department of Health and by the Information Commissioner
- The processing of personal data within the CCG is in compliance with the Regulation / Act
- Notification to the Information Commissioner (where required) of processing of personal data by the CCG is up to date
- Consulting with the Information Commissioners Office where there are high risk projects and or when there is limited scope to minimise risk
- That relevant data breaches are reported by the Data Protection Officer to the Information Commissioners Office within 72 hours of the CCG becoming aware of the breach
- Where 'consent' is the legal basis for processing personal data under GDPR the CCG will ensure there is a process in place for withdrawing that consent which is no more complex than the process of giving consent initially
- There is scheduled review of this policy

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

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.

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

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

6. PROCESS

6.1 Selected Legislation

The legislation listed below also refers to issues of security and confidentiality of personal data (more detailed description in Appendix 2):

- 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
- General Data Protection Regulation 2016
- Common Law Duty of Confidentiality (case law)

6.2 NHS and related guidance

The following are the main publications referring to security and confidentiality of personal identifiable information:

- HSCIC : Guide to Confidentiality 2013
- Employee 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
- Caldicott Report
- NHS Constitution

Further guidance can also be found via the Data Security & Protection Toolkit (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkitOverview of the General Data Protection Regulation & the Data Protection Act 2018

The GDPR was adopted by the EU in May 2016 and came in to force on 25th May 2018. The GDPR replaces the previous Directive 95/46/EC on which the Data Protection Act 1998 was based.

The DPA 2018 contains the derogations from GDPR which gives member states limited opportunities to make provisions for how it applies in their country. It is therefore important that the GDPR and the DPA 2018 are read side by side. [

The GDPR sets out specific rights for individuals and affirms that organisations must proactively assure themselves as to the use of, transfers of and legal bases for processing the information they hold. Where new uses or processes for information are introduced, these must be subject to a Data Protection Impact Assessment, and in certain circumstances approval must be obtained by the supervisory authority (the Information Commissioner) before that processing may commence.

The legislation applies to all person identifiable information held in manual files, computer databases, videos and other automated media, about living individuals. The legislation 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 or criminal prosecution.

The legislation also requires the CCG (where appropriate) to register its information held manually and on computers and other automated equipment with the Office of the Information Commissioner, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. The CCG also has to comply with the principles of good practice known as the Eight Data Protection Principles (Appendix 1). Failure to register (where appropriate), an incorrect registration or an outdated registration, are criminal offences, which may lead to prosecution of the CCG. CCG notification is maintained and reviewed annually.

Under a provision of the General Data Protection Regulation 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 (please refer to the Subject Access Request Procedure on the CCG intranet).

Please see Appendix 3 for an overview of NHS and related guidance.

6.3 Data Protection Principles

Article 5 of the GDPR requires that data controllers ensure personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

There is a requirement to appoint a Data Protection Officer

6.4 Individual Rights

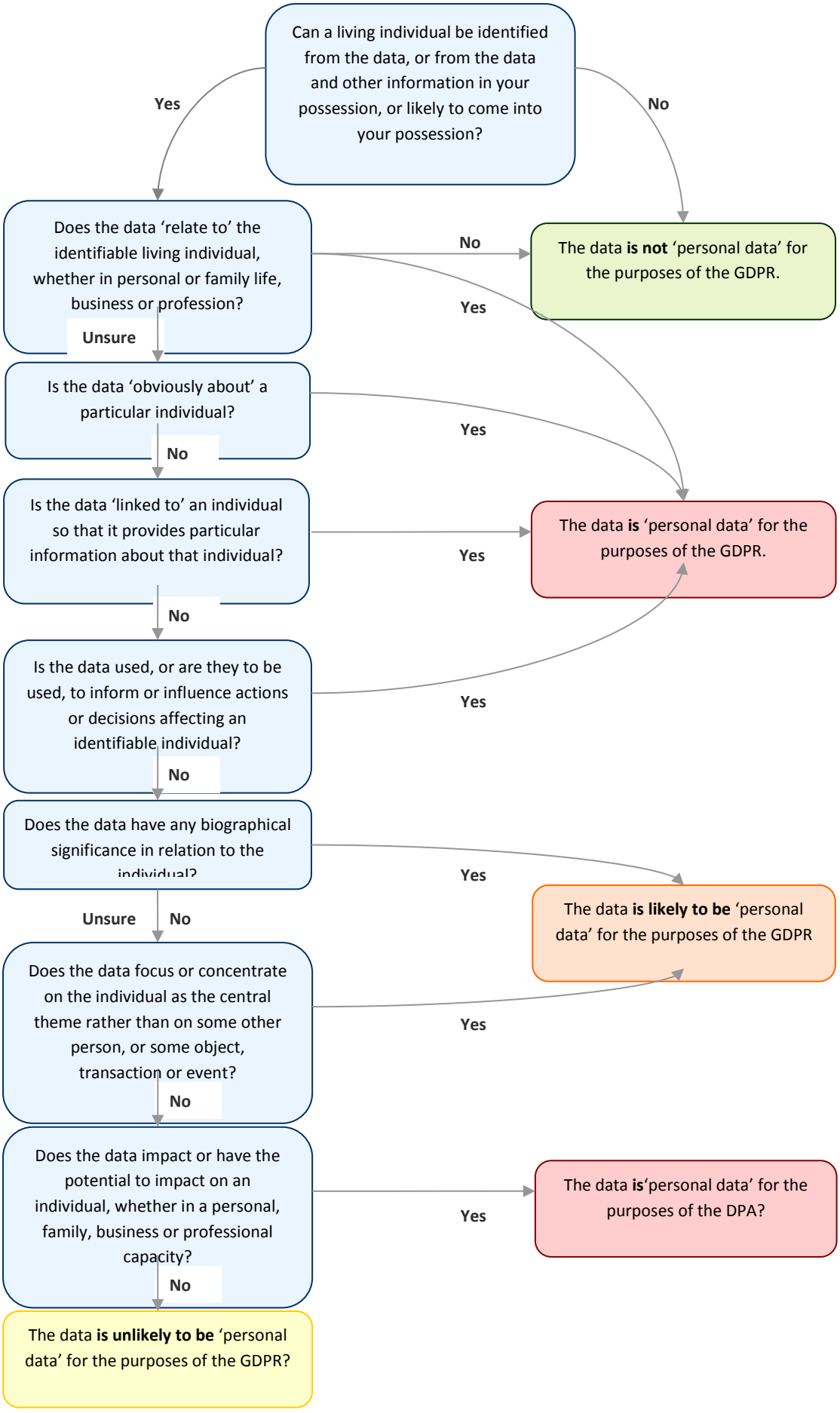
Under GDPR (Chapter III) Data Subjects have the following rights[1]:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

6.5 Determining Personal Data

The following flow chart can be used by staff to help assess when certain kinds of data may or may not constitute Personal

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/


Can a living individual be identified from the data, or from the data and other information in your possession, or likely to come into your possession?
Yes
No
Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?
No
The data **is not** 'personal data' for the purposes of the GDPR.
Yes
Unsure
Is the data 'obviously about' a particular individual?
Yes
No
Is the data 'linked to' an individual so that it provides particular information about that individual?
The data **is** 'personal data' for the purposes of the GDPR.
Yes
No
Is the data used, or are they to be used, to inform or influence actions or decisions affecting an identifiable individual?
Yes
No
Does the data have any biographical significance in relation to the individual?
Yes
The data **is likely to be** 'personal data' for the purposes of the GDPR
Unsure
No
Does the data focus or concentrate on the individual as the central theme rather than on some other person, or some object, transaction or event?
Yes
No
Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?
The data **is**'personal data' for the purposes of the DPA?
Yes
No
The data **is unlikely to be** 'personal data' for the purposes of the GDPR?

6.7 Caldicott Report Overview

Provides guidance to the NHS on the use and protection of personal confidential information (PCD), and emphasises the need for controls over the availability and access to such information. It made a series of recommendations which led to the requirement for all NHS organisations to appoint a Caldicott Guardian, who is responsible ensuring compliance with the 6 (original) Caldicott confidentiality principles.

A review of the Caldicott Principles through a 2012 review by Dame Fiona Caldicott – report "The Information Governance Review – To share or not to share" published in April 2013 added a new Principle.

The seven principles provided by the 2013 report are the baseline for good practice;

- Principle 1 – Justify the purpose(s) for using confidential information.
- Principle 2 – Only use it when absolutely necessary.
- Principle 3 – Use the minimum that is required.
- Principle 4 – Access should be on a strict need to know basis.
- Principle 5 – Everyone must understand their responsibilities.
- Principle 6 – Understand and comply with the law.
- Principle 7 – Duty to share information can be as important as the duty to protect patient confidentiality.

6.8 Staff Issues

Contracts of employment

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

Disciplinary

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.

6.9 Disclosure of personal identifiable information

There are Acts of Parliament that govern the disclosure/sharing of personal identifiable information. Some make it a legal requirement to disclose whilst others state when information cannot be disclosed. The Confidentiality: NHS Code of Practice (2003) gives clear guidance on disclosure of patient information. Some examples include:

Legislation to restrict disclosure

- Human Fertilisation and Embryology (Disclosure of Information) Act 1992

- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

Legislation requiring disclosure

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunizations and vaccinations to NHS CCGs from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

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. The Information Commissioner's Information Sharing Code of Practice provides good practice advice.

6.10 Keeping patients informed

It is a CCG and a legal 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 (Confidentiality: NHS Code of Practice 2003). 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 except in circumstances where the Common Law Duty of Confidentiality can be set aside.

6.11 Data Protection contractual clauses

The CCG is responsible for obtaining appropriate contractual assurance in respect of compliance with Information Governance (IG) requirements from all bodies that have access to the CCGs information or conduct any form of information processing on its behalf. This is particularly important where the information is about identifiable individuals as this is a legal requirement under the Data Protection Act.

All contractors or support organisations (including non-clinical staff) with access to personal data (that the CCG is data controller for) must be identified and appropriate clauses for inclusion in contracts must be developed

6.12 Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are a tool to build Data Protection Act compliance into projects and initiatives. DPIAs are legislative requirement under GDPR and are also good practice to comply with legal obligations and the CCG's use of DPIAs must be demonstrated through the NHS Data Security and Protection Toolkit.

DPIAs are intended to build in "privacy by design" and are also intended to prevent privacy related problems from arising, by:

- Considering the impact on privacy at the project start
- Identifying ways of minimising any adverse impact
- 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 should also 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 individuals

The completion of a DPIA otherwise known as a Data Protection Impact Assessment (DPIA) is mandatory under GDPR when processing is "likely to result in a high risk to the rights and freedoms of natural persons".

7 TRAINING REQUIREMENTS

Information Governance training is mandatory and all new starters who must receive IG training as part of their corporate induction. IG Training will be delivered via the NHS Digital Data Security Awareness Level 1 training module and this covers the minimum requirements. There is additional resources / training available which is role specific such as IAO training, records management and data transfers for example.

The Information Governance Framework identifies the type and frequency of training for specific roles. Additionally local face to face training may be provided where appropriate.

8 EQUALITY AND DIVERSITY

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.

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.

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 DUE REGARD

This policy has been reviewed in relation to having 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.

10 REFERENCES AND ASSOCIATED DOCUMENTATION

The Data Protection Act 1998

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Confidentiality Advisory Group - Section 251 applications

http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/

NHS Digital (formerly HSCIC) – A Guide to Confidentiality in Health & Social Care

http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

NHS Code of Practice on Confidentiality 2003 (DoH)

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

The Freedom of Information Act 2000

http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

The Human Rights Act 1998

http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Access to Health Records Act 1990

http://www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1

Caldicott review of Patient Identifiable Information 1997

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4068403

Caldicott 2 review 2013 http://caldicott2.dh.gov.uk/ (incorporating 7 Caldicott Principles)

Information Commissioner – Data Sharing Code of Practice

https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

NHS Constitution

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf

General Data Protection Regulation 2016

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

11 MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF, PROCEDURAL DOCUMENTS

Compliance with this policy will be monitored through various requirements of the CCG's Information Governance Management Framework, which are routinely reported to and monitored by, the Information Governance Committee. Relevant requirements include:

- Information Flow Mapping Registers
- Information Asset Registers
- Information Governance Contractual Arrangements
- Information Governance Incident Reports
- Privacy Impact Assessment Registers

Routine reports on Information Governance are presented to the Governance Committee.

12 APPENDICES

Appendix A: Overview of legislation

The Access to Health Records 1990

This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons' records. All other requests for access to information to living individuals are provided under the access provisions of the Data Protection Act 1998.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Human Rights Act 1998

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, CCGs, and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act came into force on 1 January 2005. This act gives individuals right of access to corporate information held by the CCG such as policies, reports, minutes of meetings. The CCG has a Freedom of Information Policy and a nominated officer to deal with requests and queries.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue individual users an individual user ID and password which will only be known by the individual they relate to and must not be divulged / misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

Appendix B: Overview of NHS Guidance

HSCIC Guide to Confidentiality 2013 This code of practice provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their health information

. It also details the required practice the NHS must follow concerning security, identifying the main legal responsibilities for an organisation and also details employee's responsibilities

Caldicott Principles

Provides guidelines relating to the sharing of patient identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance.

A review of the use of personal confidential information by Dame Fiona Caldicott updated the principles. The full report can be found here at www.gov.uk/government/publications/the-information-governance-review.

Employee Code of Practice

Guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff / employee and other individual's information

Records Management Code of Practice of Health & Social Care 2016

Provides guidance to improve the management of NHS and Social care records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS and Social care such as patients, employees, volunteers etc. Aids compliance with the Data Protection and Freedom of Information Acts

ISO/IEC 27001 / 17799 Information Security Standards

These are the accepted industry standard for Information Management and Security and have been adopted by all NHS organisations. It is also a recommended legal requirement under principle 7 of the Data Protection Act.