NHS
Nottingham and Nottinghamshire
Clinical Commissioning Group

# Confidentiality and Data Protection Policy

## 2019-2023

| | |
|---|---|
| **Version:** | 1.2 |
| **Approved by:** | Information Governance Management and Technology Committee |
| **Date approved:** | April 2019 |
| **Adopted:** | Adopted by Governing Body in April 2020 |
| **Date of issue (communicated to staff):** | April 2019 |
| **Next review date:** | March 2023 |
| **Document author:** | Head of Information Governance |

| CONTROL RECORD | | | | |
|---|---|---|---|---|
| **Reference Number**<br>N&N IG-002 | **Version**<br>1.2 | **Status**<br>Final | **Author**<br>Head of Information Governance | |
| | | | **Sponsor**<br>Associate Director of Governance | |
| | | | **Team**<br>Information Governance | |
| **Title** | Confidentiality & Data Protection Policy | | | |
| **Amendments** | Review date extension to March 2023; approved by Governing Body on 2.2.2022 | | | |
| **Purpose** | This Data Protection Policy aims to detail how the CCG meets its legal obligations and NHS requirements concerning confidentiality and information security standards | | | |
| **Superseded Documents** | Version 1.1 | | | |
| **Audience** | This policy applies to any person directly employed, contracted or volunteering to the CCG | | | |
| **Consulted with** | SIRO, Caldicott Guardian and Data Protection Officer | | | |
| **Equality Impact Assessment** | Complete – see section 14 | | | |
| **Approving Body** | Information Governance Management and Technology Committee | | **Date approved** | April 2019<br>(adopted by Governing Body in April 2020) |
| **Date of Issue** | April 2019 | | | |
| **Review Date** | March 2023 | | | |
| **This is a controlled document and whilst this policy may be printed, the electronic version available on the CCG's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.** | | | | |

**Nottingham and Nottinghamshire CCG's policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at** ncccg.team.communications@nhs.net

## Contents

## Quick Reference Guide

1) The Nottingham and Nottinghamshire Clinical Commissioning Group (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 seconders are responsible for maintaining compliance with the Data Protection Principles and reporting non-compliance through the CCG's incident reporting process.

3) Under a provision of the GDPR, an individual can request access to their personal information regardless of the form 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 either a written or verbal application to the CCG. Requests should be made in writing where possible; writing includes email. If a staff member receives a verbal request then this must be documented from the time that it is received.

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.

5) Patients must be made aware of this requirement by the use of privacy notices, 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 data they process.

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

7) Staff contracts of employment are produced and monitored by the CCG's HR Team or with HR expertise provided through a Service Level Agreement with Arden and Greater East Midlands Commissioning Support Unit. All contracts of employment include Information Governance clauses, including confidentiality 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 the CCG's policies and procedures relating to the processing of personal information.

9) There is legislation that governs the disclosure / sharing of personal or sensitive information. Some make it a legal requirement to disclose whilst others state when information cannot be disclosed.

10) NHS Digital (formerly HSCIC) Guide to Confidentiality 2013 gives clear guidance on disclosure of patient information further advice should always be sought from the CCG's Information Governance Lead.

11) Whilst there is a public expectation of appropriate sharing of information between organisations providing health care 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.

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

13) Where a Data Protection Impact Assessment identifies a high risk that cannot be mitigated, the CCG will consult the ICO before starting the processing.

14) 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 personal confidential data can be held, received and communicated securely.

15) Information Asset Owners are required to ensure there is a documented policy for approvals and authorisation for mobile working and teleworking arrangements. They are responsible for undertaking information security risk assessments for each of the CCG's Information Assets for which they are responsible 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 personal confidential data.

16) 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.

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

18) 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. Introduction

Nottingham and Nottinghamshire CCG (hereafter referred to as '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 its employees for non-compliance with relevant legislation and NHS guidance.

## 2. 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. The requirements are primarily based upon key pieces of legislation, the Data Protection Act 2018 and the EU General Data Protection Regulation 2016; however, other relevant legislation and appropriate guidance will be referenced.

## 3. Scope

This policy applies to all CCG employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers), including Governing Body and lay members. Third Parties will be governed by any associated information sharing agreements and will be made aware of this policy.

The policy also applies to any person directly employed, contracted by or volunteering for the CCG.

## 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/her] agreement to personal data relating to [him/her] being processed'.

**Data Controller**: The person or organisation that collects personal data and decides on how to use, store and 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**: A living individual who is the subject of the personal data.

**Personal Confidential Data:** This is personal information about identified or identifiable individuals which is also confidential. 'Personal' includes the Data Protection Act definition of personal data, but it also includes the deceased as well as the living. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' eg. health records. It is adapted to include 'special categories' data as defined in the Data Protection Act.

**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 or data processor (for example name address, postcode, NHS Number).

**Pseudonymised Information:** Information which has had identifiers removed or replaced. This is still personal data for the purposes of GDPR.

**Special Category 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, genetics, sex life, sexual orientation, criminal proceedings, convictions or biometrics (where used for ID purposes).

**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 records.

**Data Subjects** 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 Data Protection Act 2018 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 (formerly 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.

## 5. Duties and Responsibilities

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

### 5.1 Chief Executive /Accountable Officer

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 role is supported.

### 5.2 CCG

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

- All staff dealing with personal confidential data are aware of the need for compliance with the Act and associated provisions;
- There is Senior Health Professional appointed as Caldicott Guardian to oversee the processing of personal confidential data.
- All staff are also aware of the requirements of the Common Law Duty of Confidentiality as set out in the NHS Code of Practice on Confidentiality 2003 and the HSCIC/NHS Digital Guide to Confidentiality 2013;
- There is a Senior Information Risk Owner (SIRO) appointed to take ownership of organisational risk.
- 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;
- The processing of personal data within the CCG is in compliance with the Act;
- Notification to the Information Commissioner (where required) of processing of personal data by the CCG is up-to-date;
- 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; and
- There is a scheduled review of this policy.

### 5.3 Caldicott Guardian

The Caldicott Guardian is responsible for overseeing the development and implementation of CCG policies and procedures designed to ensure that all routine use of personal confidential data is identified, documented and monitored.

### 5.4 Data Protection Officer (DPO)

The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and to advise the CCG on its obligations under Data Protection Legislation.

### 5.5 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of information risk including those relating to confidentiality and data protection compliance.

### 5.6 Information Asset Owners

Information Asset Owners are responsible for understanding and addressing Information Governance risks relevant to the "information assets" that they own and are responsible for ensuring that the policy and its supporting standards and guidelines are built in to local processes and that there is on-going compliance.

### 5.7 All Managers

All managers are responsible for ensuring that their staff receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance.

### 5.8 All staff

All staff must adhere to the CCG's 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 Legislation

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

- 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;
- Privacy and Electronic Communications Regulations 2003;
- Regulation of Investigatory Powers Act 2000;
- General Data Protection Regulation (GDPR);
- Common Law Duty of Confidentiality (case law);
- The Heath & Social Care (National Data Guardian Act) 2018.

### 6.2 NHS and Related Guidance

The following are the main publications referring to security and confidentiality of personal confidential data:

- Caldicott Review 2013;
- Employee Code of Practice (Information Commissioner);
- HSCIC (now NHS Digital): Guide to Confidentiality 2013;
- ISO/IEC 27001:2005 and 17799:2005 Information Security Standard;
- NHS Constitution 2015;
- Records Management Code of Practice for Health and Social Care 2016;
- NHS Constitution;
- Data Sharing Code of Practice (Information Commissioner);
- Subject Access Code of Practice (Information Commissioner);
- Anonymisation - Managing Data Protection Risk (Information Commissioner);
- NHS Digital - Data Security Standards;

Further guidance can also be found via Data Security & Protection Toolkit https://www.dsptoolkit.nhs.uk/

### 6.3 Overview of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018

The GDPR was adopted by the EU in May 2016 and came in to force on 25 May 2018. The GDPR replaces the previous Directive 95/46/EC upon 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 (DPIA), and in certain circumstances approval must be obtained by the supervisory authority (the Information Commissioner) before that processing may commence.

The Act also 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 when it is fair and lawful to do so. 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 Act also requires the CCG (where appropriate) to register information held manually and on computers and other automated equipment with the Information Commissioner's Office, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. 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 by the IG Team and reviewed annually. A fee is paid as part of this registration process.

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's intranet).

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

### 6.4 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."

### 6.5 Individual Rights

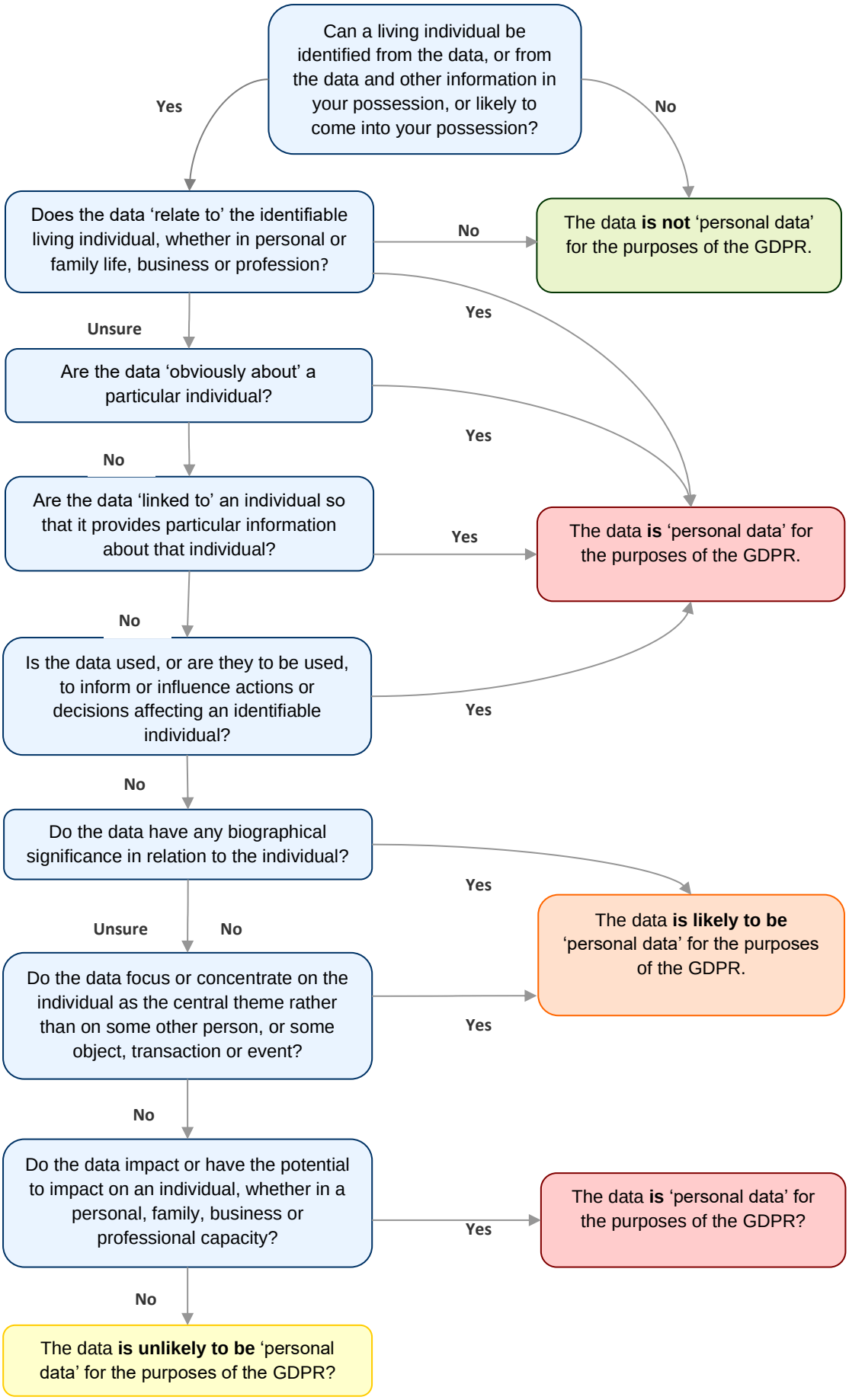
Under GDPR (Chapter III) Data Subjects have the following rights[1]

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 to processing;
8. Rights in relation to automated decision making and profiling.

### 6.6 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 Data.

[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
Are the data 'obviously about' a particular individual?
Yes
No
Are the data 'linked to' an individual so that it provides particular information about that individual?
Yes
The data **is** 'personal data' for the purposes of the GDPR.
No
Is the data used, or are they to be used, to inform or influence actions or decisions affecting an identifiable individual?
Yes
No
Do 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
Do 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
Do the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?
Yes
The data **is** 'personal data' for the purposes of the GDPR?
No
The data **is unlikely to be** 'personal data' for the purposes of the GDPR?

### 6.7 Caldicott Report

Provides guidance to the NHS on the use and protection of personal confidential information, 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 six (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.

### Caldicott Principles

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 Common Law Duty of Confidentiality

All NHS Bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional and ethical standards of confidentiality. A duty of confidence arises when a person discloses information to another (e.g. patient to clinician or employee to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law and a requirement established in professional codes of conduct.

In summary, information cannot be disclosed further unless one or more of the following applies;

- 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;

- 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; or
- Explicit or implied consent.

**Consent**

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

- **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 an individual 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 GDPR.

### 6.9 Disclosure of Personal Confidential Data

There are Acts of Parliament that govern the disclosure/sharing of person-identifiable information. Some make it a legal requirement to disclose whilst others state when information cannot be disclosed. Some examples include:

Legislation to restrict disclosure:

- Abortion Act 1967;
- Adoption Act 1976;
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992; and
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992.

Legislation requiring disclosure:

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

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 2018, the General Data Protection Regulation, the Human Rights Act 1998, the Caldicott Review Principles and the Common Law Duty of Confidentiality are upheld. Information sharing protocols facilitate the exchange of information between organisations.

### 6.10 Keeping patients informed

It is a CCG and legal requirement that patients are informed how their information is to be used before they are asked to provide it. Where personal information is obtained other than directly from the patient the patient must be provided with privacy information within a reasonable period and no later than one month.

### 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 CCG's information or conduct any form of information processing on its behalf. This is particularly important where the information is about identifiable individuals. This is a legal requirement under the General Data Protection Regulation. 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. They are a legal requirement under GDPR; the CCG's use of DPIAs is assessed through Standards of the Data Security & 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 start of a project;
- Identifying ways of minimising any adverse impact;
- Building in "privacy by design" 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 Personal Confidential Data including pseudonymised information;
- Introduce a new process that requires the use of Personal Confidential Data where it had previously been conducted anonymously;

- Involve a change in how the CCG will handle either (a) large amounts of Personal Confidential Data about an individual, or (b) Personal Identifiable Data about a large number of individuals.

The completion of a DPIA is mandatory under GDPR when processing is “likely to result in a high risk to the rights and freedoms of natural persons”

Where a high risk is identified that the CCG cannot mitigate, the CCG’s DPO is required to notify/consult with the ICO.

## 7. Training Requirements

Information Governance training is mandatory and all new starters must receive IG training as part of their corporate induction.

All staff members are required to undertake accredited Information Governance training as appropriate to their role. The preferred method is through the e-learning module available through the Electronic Staff Record (ESR) “Data Security Awareness Level 1“.

The CCG has other methods of accessing accredited training:

1. e-LfH;
2. Workbook and Assessment;
3. Classroom training (PowerPoint presentation).

Information Governance training must be completed on an annual basis. In order to achieve competency, staff will have to pass an awareness assessment as part of the training.

The CCG’s SIRO, Deputy SIRO, Caldicott Guardian, Deputy Caldicott Guardian, Information Asset Owners (IAO) and Information Asset Administrations (IAA) may require specific additional training depending on the role they hold. The identified roles requiring additional training and frequency of the training will be set out in the CCG’s training needs analysis.

## 8. Staff Issues

A breach of Data Protection legislation 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.

## 9. Interaction with Other Policies and Procedures

This policy should be read in conjunction with relevant sections of the following CCG’s policies/supporting procedures.

- Information Governance Management Framework;

- Data Protection by Design Framework;
- Information Security Policy;
- Records Management Policy;
- Freedom of Information and Environmental Information Regulations Policy;
- Electronic Remote Working Policy;
- Internet and Electronic Mail Use Policy;
- Network Security Policy;
- Data Quality Policy.

## 10. References and Associated Documentation

- Access to Health Records Act 1990 http://www.legislation.gov.uk/ukpga/1990/23/contents;
- Confidentiality Advisory Group - Section 251 applications http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/;
- Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- General Data Protection Regulation(GDPR) - https://eurlex.europa.eu/eli/reg/2016/679/oj
- Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents;
- A Guide to Confidentiality in Health and Social Care 2013 http://content.digital.nhs.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf;
- Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents;
- Information: To share or not to share? The Information Governance Review 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf;
- Review of Patient-Identifiable Information 1997 http://webarchive.nationalarchives.gov.uk/20130124064947/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf.

## 11. Monitoring Compliance

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

- Data Flow Mapping Registers;
- Information Asset Registers;

- Information Governance Contractual Arrangements;
- Information Governance Incident Reports; and
- Data Protection Impact Assessment Registers.

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

## 12. Equality and Diversity Statement

The Nottingham and Nottinghamshire CCG pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, both as a commissioner and an employer.

As a commissioning organisation, we are committed to ensuring our activities do not unlawfully discriminate on the grounds of any of the protected characteristics defined by the Equality Act, which are age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

We are committed to ensuring that our commissioning activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, roma and travellers.

As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

## 13. 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.

## 14. Equality Impact Assessment

| **Date of assessment:** | April 2019 | | | | |
|---|---|---|---|---|---|
| **For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:** | Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity? | If yes, are there any mechanisms already in place to mitigate the adverse impacts identified? | Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned. | Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe. | |
| **Age**[2] | No | N/A | N/A | No | N/A |
| **Disability**[3] | No | N/A | N/A | No | N/A |
| **Gender reassignment**[4] | No | N/A | N/A | No | N/A |
| **Marriage and civil partnership**[5] | No | N/A | N/A | No | N/A |
| **Pregnancy and maternity**[6] | No | N/A | N/A | No | N/A |

[2] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

[3] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

[4] The process of transitioning from one gender to another.

[5] Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[6] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

| **Date of assessment:** | April 2019 | | | | |
|---|---|---|---|---|---|
| **For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:** | Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity? | If yes, are there any mechanisms already in place to mitigate the adverse impacts identified? | Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned. | Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe. | |
| **Race**[7] | No | N/A | N/A | No | N/A |
| **Religion or belief**[8] | No | N/A | N/A | No | N/A |
| **Sex**[9] | No | N/A | N/A | No | N/A |
| **Sexual orientation**[10] | No | N/A | N/A | No | N/A |
| **Carers**[11] | No | N/A | N/A | No | N/A |

[7] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

[8] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

[9] A man or a woman.

[10] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[11] Individuals within the CCG which may have carer responsibilities.

## 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 a deceased person's 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.

**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.

**The Justice and Coroners Act**

This Act has amended the Data Protection Act to strengthen the Information Commissioner's inspection powers.

## Appendix B: Overview of NHS Guidance

HSCIC/NHS Digital: Guide to Confidentiality 2013. This code of practice provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their personal confidential data. 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.

**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.

**The Caldicott Principles**

A review of the use of personal confidential data by Dame Fiona Caldicott updated the previous principles. The full report provides guidelines relating to sharing of patient identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance.

**Records Management Code of Practice for Health and Social Care 2016**

Provides guidance to improve the management of NHS 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 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 standards 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.