NHS
Harrogate and Rural District
Clinical Commissioning Group

# Data Protection and Confidentiality Policy

## November 2017

| | |
|---|---|
| **Authorship:** | **Chris Wallace –**<br>**Information Governance Manager** |
| **Committee Approved:** | Audit Committee |
| **Approved date:** | November 2017 |
| **Review Date:** | November 2020 |
| **Equality Impact Assessment:** | Completed |
| **Target Audience:** | Council of Members, Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract |
| **Policy Number:** | 030 |
| **Version Number:** | 2.0 |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.**

## POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

| New Version Number | Issued by | Nature of Amendment | Approved by & Date | Date on Intranet |
|---|---|---|---|---|
| 0.1 | Chris Wallace | First draft for comments | NR | |
| 0.2 | Barry Jackson | Small amendments | NR | |
| 1.0 | H. Sanderson | Addition of HSCIC Guidance and Caldicott 2 requirements | Audit Committee March 2016 | |
| 2.0 | IG Officer | • Updated for Changes in Relationship to Embed<br>• Updates to reflect General Data Protection Requirement. | Audit Committee November 2017 | January 2018 |

**CONTENTS**

# 1 INTRODUCTION

**1.1.** The Harrogate and Rural District Clinical Commissioning Group (from this point on known as the CCG) as part of NHS England, a public body, has a statutory duty to safeguard the confidential information it holds. The principle of this policy is that no individual or company working for or with the CCG shall misuse any information it processes or comes into contact with, or allow others to do so. It is also required that all individuals or companies working for or on behalf of the CCG implements appropriate information security to protect the information they process and hold in line with legal obligations and NHS requirements.

**1.2.** During the course of their day to day work, many individuals working within or for the CCG will often handle or be exposed to information which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company and firm to which this policy applies shall not at any time during the period they work for or provide services to the CCG or at any time after its termination, disclose confidential information that is held or processed by or on behalf of the CCG.

**1.3** All staff working in the CCG are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act Legislation and, for health and other professionals, through their own professions Codes of Conduct.

**1.4.** The CCG places great emphasis on the need for the strictest confidentiality in respect of person identifiable and sensitive data. This applies to manual and computer records and conversations about service user's treatments. Everyone working for the CCG is under a legal duty to keep service user's information, held in whatever form, confidential. Service users who feel that confidence has been breached may issue a complaint under the CCG complaints procedure or they could take legal action.

**1.5.** Confidentiality should only be breached in exceptional circumstances and with appropriate justification and this must be fully documented.

**1.6.** The CCG is committed to the delivery of a first class confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information where necessary;
- gain trust in the way the CCG handles information; and
- understand their rights to access information held about them.

## 2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

## 3 IMPACT ANALYSES

### 3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

### 3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

## 4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc

**4.1.** For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

**4.2.** For the purposes of this policy, confidential information shall include any confidential information relating to the CCG and/or its agents, customers, prospective customers, service users, suppliers or any other third parties connected with the CCG and in particular shall include, without limitation:

- service user information;
- ideas/programme plans/forecasts/risks/issues;
- finance/budget planning/business cases;
- sources of supply and costs of equipment and/or software;
- prospective business opportunities in general;
- computer programs and/or software adapted or used;
- corporate or personnel information; and
- contractual and confidential supplier information. This is irrespective of whether the material is marked as confidential or not.

## 5 POLICY PURPOSE & AIMS

The aims of this policy are:

- to safeguard all confidential information held and processed by the CCG;
- to ensure the CCG has identified a legal basis for holding and processing personal identifiable information;
- to complete privacy impact assessments on all new ways of processing personal identifiable information;
- to ensure appropriate information sharing agreements are in place for information sharing;
- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to confidentiality across the CCG;
- to ensure all staff are aware of their responsibilities with regards to confidential information;
- to provide all individuals working within the CCG access to the documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them. These include:
  - the common law duty of confidentiality;
  - Caldicott principles;
  - Human Rights Act 1998;
  - the Department of Health Publication: Confidentiality: NHS Code of Practice November 2003;
  - HSCIC: Code of Practice on confidential information;
  - HSCIC: A guide to confidentiality in health and social care;
  - the Department of Health Publication Confidentiality: NHS Code of Practice – Supplementary Guidance: Public Interest Disclosures November 2010;
  - Data Protection Act 1998;
  - General Data Protection Regulation 2016
  - The Public Interest Disclosure Act 1998;
  - Health and Social Care Act 2012 and HSC (Safety and Quality) Act 2015.
  - The Computer Misuse Act 1990;
  - Care Record Guarantee.
  - Information Commissioners Data Sharing Code of Practice

It must also be recognised that under the Data Protection Act Legislation that individuals have the right to request access to their information, regardless of the media and format in which the information is held. The CCG must therefore put processes and procedures in place to respond to subject access requests in line with current Data Protection ActLegislation, the CCG has documented and published a policy for dealing with subject access requests

### 5.1 Direct Marketing (Privacy & Electronic Communications Regulations)

The Privacy and Electronic Communications Regulations (PECR) set out detailed rules and legal requirements in a number of areas that apply to direct marketing of services and products. The marketing rules apply if you are sending marketing and advertising by electronic means, such as by

telephone, fax, email, text, picture or video message, or by using an automated calling system.

The relationship between PECR and the Data Protection Legislation is a complex one and staff who intend to carry out marketing activities on behalf of the organisation need to be aware of these regulations. Guidance on this is attached with a link to the Information Commissioner's Office and the regulations. See Privacy and Electronic Communications Regulations attached at Appendix 1.

**5.2 Conduct**

Individuals shall not be restrained from using or disclosing any confidential information which:

- they are authorised to use or disclose by the CCG; and/or
- has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure by the individual; and/or
- has entered the public domain by an authorised disclosure for an authorised purpose by the individual or anyone else employed or engaged by the CCG; and/or
- they are required to disclose by law; and/or
- they are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regard to the provisions of that Act.

NB/ Disclosures should be in accordance with a relevant information sharing agreement, unless the disclosure is required by law, including under the Public Interest Disclosure Act 1998. The HSCIC have published a Code of Practice on confidential information and A Guide to Confidentiality in Health and Social Care which give comprehensive guidance in handling and sharing confidential information for different purposes.

All individuals must:

- exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- ensure the physical security of all confidential documents and/or media, including storage of files on PCs and any mobile equipment. Confidential information must never be left unattended and should be secure when not in use;
- password protect all magnetic media
- passwords must not be disclosed to anyone including colleagues.
- Only use officially issued and fully encrypted mobile equipment in line with the mobile/agile working standard.
- Individuals must implement appropriate information security and safe haven procedures to protect the information they hold and process

All individuals will be required to comply with this policy whilst working within the CCG and thereafter for as long as the information remains confidential information. It is only when the information has entered the public domain that the information can be classed as no longer confidential.

If an individual is unclear if information should be classified as confidential, they must discuss the issue with their manager who will offer advice.

### 5.3. The duty of confidence

- 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 ethical standards of confidentiality.
- Everyone working for or with the NHS records that handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his/her employer.
- The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.
- Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff includes those who are not involved in either the clinical care of the service user or the associated administration processes.
- No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).
- No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.
- Service users are entitled to object to the use of their personal health data for purposes other than their immediate care.
- The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

### 5.4. What is personal information

- Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, pseudonymised data, biometric and genetic data, and online identifiers and location data,etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.
- Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary.
- Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.

- Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.
- Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information regarding race, health, sexuality, etc.
- Confidential information may be known, or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

### 5.5. Disclosing information

- The HSCIC Code of Practice on Confidential Information and The Guide to Confidentiality in Health and Social Care Services provide advice on using and disclosing confidential service user information and have models for confidentiality decisions and all staff should adhere to this guidance.
- Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.
- The CCG will inform service users, staff and any other data subject why, how and for what purpose personal information is collected, recorded and processed by means of a privacy notice on the CCG website and where necessary service user information leaflets.
- Consent of the data subject will be required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional. This consent must be recorded.
- Under common law, personal information may be disclosed without consent for example:
    - in order to prevent abuse or serious harm to others
    - where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.
- Where information is required by the police, this must be in line with the Data Protection Act section 29, and staff should consult the Information Governance, Security and Compliance Manager. Decisions on whether to disclose information or not must be recorded.

### 5.6 Personnel information

In keeping with good Human Resources practice, the CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process “sensitive personal data” (as defined by the Data Protection Legislation), for example in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring for the prevention of fraud or other illegal activities.

The CCG may process such data and such data may be legitimately disclosed to appropriate employees and to the CCG professional advisors, in accordance with the principles of the Data Protection Legislation.

The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her is or may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the Head of Human Resources.

### 5.7. Media enquiries

All requests for information by the media, other than those made under the Freedom of Information (FOI) Act, must be referred to the Communications Team.

### 5.8. Termination or expiry of a contract with the CCG

On leaving or termination of a contract with the CCG any copies of software, documents or correspondence, diaries, documents, plans, specifications or any other information relevant to the CCG (whether or not prepared or produced by the individual) must be returned to the CCG's possession and under no circumstances must the leaver take this information with them. All individuals that have left the CCG are bound by the Confidentiality Policy that was in publication at the time of their departure.

### 5.9. Awareness and compliance

It is important to the CCG to protect its legitimate business interests and in particular it's confidential information. Breaches of confidentiality, of any sort, including breach of this policy will be regarded as serious misconduct and may result in:

- dismissal;
- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures;
- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and
- legal action being taken against the discloser and/or any other third party.

If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and/or to the CCG HR Directorate.

Everyone in the CCG must be aware of the importance of confidentiality. All staff need to be aware of their responsibilities for safeguarding service user confidentiality and keeping information secure.

The duty of confidentiality is written into employment contracts. Breaches of confidentiality are a serious matter. A breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence which could result in dismissal and/ or prosecution. No employee shall knowingly misuse any information or allow others to do so.

It is a disciplinary offence to access records/ information that you have no legitimate reason to view this includes, records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

## 6 ROLES / RESPONSIBILITIES / DUTIES

**6.1.** Overall accountability for procedural documents across the organisation lies with the Managing Director who has overall responsibility for establishing and maintaining an effective Information Governance Framework, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

**6.2.** Overall responsibility for the confidentiality policy lies with Information Governance, Security & Compliance manager who has delegated responsibility for managing the development and implementation of Confidentiality policy procedural documents.

**6.3.** The Caldicott Guardian is responsible for overseeing and advising on issues of service user confidentiality for the CCG.

**6.4.** Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

**6.5.** Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the CCG and this extends after they have left the employ of the CCG.

**6.6.** Individual staff members are personally responsible for any decision to pass on information that they may make.

**6.7.** All staff are responsible for adhering to the Caldicott principles, Data Protection Legislation , and the Confidentiality Code of Conduct.

**6.8.** Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings);
- staff Intranet;

**6.9.** All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Statutory and Mandatory Training Standard and Information Governance Training Needs Analysis.

**6.10.** The CCG must ensure that all contractors and supporting organisations are working to documented contracts or service level agreements that detail their responsibilities in respect of information governance and security, and confidentiality and data protection. This includes the completion of the Information Governance Toolkit to a minimum of level 2 compliance.

## 7 IMPLEMENTATION

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

*'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.*

## 8 TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet.

## 9 MONITORING & AUDIT

**9.1.** Performance against the Information Governance Toolkit will be reviewed on an annual basis and used to inform the development of future procedural documents.

**9.2.** This policy will be reviewed regularly, and in accordance with the following on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

**9.3.** Equality Impact Assessment

**9.3.1.** The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, service users and the public have been reviewed in line with the CCG's Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, service users and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/ belief.

**9.3.2.** The Equality Impact Assessment has been completed and has identified impact or potential impact as "no impact"

### 9.4. Records Management, Retention and Disposal

**9.4.1.** A records management system must be implemented to ensure that all records are maintained in accordance with the Data Protection Legislation and Caldicott Principles (See Annexes A&B), and the NHS Records Management, Code of Practice.

**9.4.2** The records management systems must include appropriate controls to protect information from unauthorised access, theft or loss, and inappropriate disclosure of person identifiable or corporately confidential information.

**9.4.3** A system of timely housekeeping must be implemented and include secure methods of destruction for records that have reached their retention period and been assessed as not to be retained for permanent preservation.

### 9.5. Complaints

**9.5.1** The CCG will implement a complaints procedure to deal with complaints in connection with the Data Protection Act and breaches of confidentiality. If the complainant is not satisfied with the investigation and outcome of their complaint they should be advised of their right to contact the Information Commissioners Office.

## 10 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

## 11 REFERENCES

**11.1.** A set of procedural document manuals will be available via the CCG staff intranet.

**11.2.** Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff intranet.

**11.3**. All documents in the CCG Policies and Procedures Register are relevant.

**Appendix 1**

| 1. Equality Impact Analysis | |
|---|---|
| **Policy / Project / Function:** | Data Protection and Confidentiality policy |
| **Date of Analysis:** | 13/01/14 |
| **This Equality Impact Analysis was completed by:**<br>**(Name and Department)** | C Wallace - IG Manager – CSU IG Team |
| **What are the aims and intended effects of this policy, project or function ?** | This policy sets out the CCG's responsibilities under the Data Protection act and provides guidance on how information held by the organisation should be treated and were necessary kept confidential. |
| **Please list any other policies that are related to or referred to as part of this analysis?** | |
| **Who does the policy, project or function affect ?**<br><br>Please Tick ✔ | Employees ☒<br>Service Users ☐<br>Members of the Public ☐<br>Other (List Below) ☐ |

| 2. **Equality Impact Analysis: Screening** | | | | | |
|---|---|---|---|---|---|
| | Could this policy have a positive impact on… | | Could this policy have a negative impact on… | | Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact |
| | Yes | No | Yes | No | |
| **Race** | ☐ | ☒ | ☐ | ☒ | |
| **Age** | ☐ | ☒ | ☐ | ☒ | |
| **Sexual Orientation** | ☐ | ☒ | ☐ | ☒ | |
| **Disabled People** | ☐ | ☒ | ☐ | ☒ | |
| **Gender** | ☐ | ☒ | ☐ | ☒ | |
| **Transgender People** | ☐ | ☒ | ☐ | ☒ | |
| **Pregnancy and Maternity** | ☐ | ☒ | ☐ | ☒ | |
| **Marital Status** | ☐ | ☒ | ☐ | ☒ | |
| **Religion and Belief** | ☐ | ☒ | ☐ | ☒ | |
| **Reasoning** | | | | | |
| **If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7** | | | | | |