Cambridgeshire and Peterborough
Clinical Commissioning Group (CCG)

# CONFIDENTIALITY CODE OF CONDUCT FOR EMPLOYEES 2021-2023

**Ratification Process**

| | |
|---|---|
| Lead Authors: | Information Governance Lead/DPO<br>Information Governance Manager |
| Developed by: | Information Governance Team |
| Approved by: | Information Governance, Business Intelligence & IM&T Steering Group 15th July 2021 |
| Endorsed by: | Integrated Performance and Assurance Committee 24th August 2021 |
| Ratified by: | CCG Governing Body 7th September 2021 |
| Version: | 5.0 |
| Latest Revision date: | July 2023 (or earlier if significant change to local or national requirements) |
| Valid on: | 7th September 2021 |

**Document Control Sheet**

| | |
|---|---|
| Development and Consultation: | Policy developed in consultation with the IG, BI and IM&T Steering Group and endorsed by the Clinical Executive Committee. |
| Dissemination | The Human Resources and Corporate Governance Teams will be made aware of the Policy review and update for referencing / inclusion in induction papers. All staff within the CCG will be notified of the via the weekly staff comms. |
| Implementation | The Caldicott Guardian is responsible for monitoring the application of the policy by ensuring that:<br>• The policy is brought to the attention of all employees;<br>• Managers are aware of their responsibilities for ensuring that staff under their control implement the policy;<br>• Staff are informed and consulted as appropriate;<br>• Appropriate training and guidance is provided to staff;<br>• Corporate business processes support the implementation of the policy. |
| Training | Training will be undertaken as part of the CCG's ongoing processes. |
| Audit | Implementation of the Policy will be monitored on a regular basis. |
| Review | This policy will be reviewed two yearly, or earlier if there are changes in procedures or legislation. |
| Links with other Documents | The Policy should be read in conjunction with the following CCG Policies:<br>• IG Policy and Management Framework<br>• Information Security for Staff Policy<br>• Safe Haven Policy<br>• Removable Media Policy<br>• Records Management and Lifecycle Policy (Sections 17 & 20 - Disposal of Records)<br>• Ways of Working Policy and Procedure<br>• Standards of Business Conduct & Commercial Sponsorship Policy<br>• Conflicts of Interests Policy |
| Equality and Diversity | The OD & HR Advisor (Equality and Diversity) carried out an Equality & Diversity Impact assessment (Annex A) and concluded the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found. |

**Revisions**

| Version | Page/ Para No | Description of change | Date approved |
|---|---|---|---|
| 1.0 | | Developed as CCG policy from an existing PCT policy. Web link to Information Sharing Framework hosted by Cambridgeshire County Council website. Health and Social Care Act 2012 referenced. | April 2013 |
| 1.1 | Links with other DtGP 4.3 | Replaced Email AUP with Information Security Staff Policy | |
| 2.0 | Whole document overview | Reviewed and ratified by CMET following policy expiry | July 2015 |
| 3.0 | Whole document overview | Reference to national Code of practice on confidential information 2014 and Health and Social Care Act 2012 included | July 2017 |
| 3.1 | Document Control Sheet | Reviewed and updated to align with / reference the CCG's Standards of Business Conduct and Commercial Sponsorship Policy and Conflicts of Interest Policy.<br>CCG Caldicott Guardian updated. | April 2018 |
| 4.0 | Whole document overview | Reviewed and updated. Confidentiality, Integrity, Availability (CIA) incorporated according to the requirements of the Data Protection Act 2018 and Data Security and Protection Toolkit. | 27th Aug 2019 |
| 5.0 | Whole document review | Section 2.1 CIA – Additional detail included regarding the UK GDPR Security Principle.<br>Section 4.2 – Faxing, revised to reflect new NHS requirement from April 2020.<br>Section 7 – Reminder to staff added regarding not storing their password or pin number alongside CCG issued equipment.<br>Section 8 – Confidentiality whilst Working at Home, section revised referencing the CCG's new Working Practices and Standards of Business Etiquette Policy and Procedure. | 15th July 2021 |

**Contents**

## CODE OF CONDUCT FOR EMPLOYEES IN RESPECT OF CONFIDENTIALITY

**This document should be read and understood prior to the contract of employment or other confidentiality agreement being signed. If there is anything that is not clear, please contact your line manager.**

### 1 Purpose of the Code

1.1 This policy details required practice for those who work within or under contract to the CCG concerning maintaining confidentiality for all personally identifiable information. For the purposes of this document the term 'employee' is used as a convenience to refer to all those to whom this code should apply. Whilst directed at CCG staff it is also relevant to anyone working in and around the CCG to include contractors, agency staff, students and volunteers.

1.2 All employees working in the NHS are bound by a statutory duty of confidence to protect personal information. This is a requirement within:

- The Data Protection Act 2018
- The Human Rights Act 1998 (Article 8)
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988
- Health and Social Care Act 2012
- Code of Practice on Confidential Information

In addition, for clinical and other professional staff the requirement is contained within their own professional Code(s) of Conduct. (Appendix 2)

1.3 This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that a limited number of employees (e.g. Complex Case; Exceptional Case and Patient Experience Teams) also come into contact with other confidential information which should also be treated with the same degree of care e.g. business in confidence information.

1.4 The principle behind this Code of Practice ('Code') is that no employee shall knowingly breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the CCG security systems or controls in order to do so.

1.5 This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. Breach of confidentiality of information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal. (See Appendix 3)

1.6 Any organisation that collects, analyses, publishes or disseminates confidential health and care information must follow the Code of practice on confidential information. It clearly defines the steps that organisations must take to ensure that confidential information is handled appropriately. The Code provides good practice guidance that helps organisations put the right structures and procedures in place to ensure that its employees follow confidentiality rules.

## 2 Definitions

See also Glossary of Terms – Appendix 1

### 2.1 Confidentiality, Integrity and Availability (CIA)

A key principle of the UK GDPR is that organisations process personal data securely by means of 'appropriate technical and organisational measures' – this is known as the 'security principle'. Organisations are required to implement measures to ensure the 'confidentiality, integrity and availability' of their systems and services and the personal data that is processed within them.

All CCG employees are responsible for maintaining the **C**onfidentiality, **I**ntegrity and **A**vailability of personal data.

**Confidentiality** is about privacy and ensuring that information is only accessible to those who have a proven need to see it.

**Integrity** is about information being accurate and up to date.

**Availability** is about information being there when it is needed to support care.

### 2.2 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

Information may be held in paper or electronic format, computer file or printouts, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops; mobile phones; removable media; recording devices and digital cameras etc.

It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any company e.g. CCG business confidential 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 or online identifiers (including IP addresses and cookie identifiers) etc. A visual image (e.g. photograph) can be sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated within legislation. Under the Data Protection Act 2018, this type of data is now known as 'Special Category' data and relates to data about an individual's race; ethnic origin; politics; religion; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation etc.

During your duty of work, you should consider all information to be sensitive, even something as a simple as a patient's name and address. The same standards should be applied to all information you come into contact with.

### 2.3 Ensuring that the data subject understands how their information will be used

Staff and data subjects (or their representatives) must understand how we will use information about them. Achieving this understanding will therefore depend on staff giving the data subject relevant information about the purposes of processing information about them and any likely disclosures. A Confidentiality Statement should be completed with the data subject, and they should be asked to sign to confirm their understanding and agreement. The practitioner responsible for the care of the service user *must* discuss the uses of their information with them. The CCG's Privacy and Fair Processing Notice on the public website outlines what information the CCG holds and how we use it. Leaflets can also be useful for reinforcing information given to a person but are not in themselves sufficient. As a minimum, any explanation provided should include:

- That the main use of the information will be to manage the data subject's care and treatment, and that it is very important that we have full and accurate information if we are to provide the best care.

- That we also use their information to check the quality of the care that they and other service users receive, to ensure that this is of the right standard. This process is called audit. Everyone involved in audit must follow the same strict rules on confidentiality.

- That you work as part of a team and will share information about the data subject with the team if it is necessary to provide the best care for them. Explain who is a member of your team. If you work with members of another agency then you should explain that information may be passed to that agency if it is necessary to provide their care, but that the agency has also signed up to the same standards of confidentiality.

- That data subjects have a 'right of access' to their health records. This is commonly referred to as subject access and gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully. More information regarding Subject Access Requests, can be found within the CCG's Access to Records Policy, available on the public website here. Any requests for access to records received must be forwarded to the Information Governance Team who will respond on behalf of the CCG unless it has been formally agreed that your team will handle them.

- That we send anonymous information to the NHS Digital to allow us to manage services and monitor effectiveness. NHS Digital play a major role in handling data for health and social care; the data that they collect helps to improve patient care.

- It may also be appropriate or necessary to discuss the use of the subject's information at other times during their care, for example:

- When transferring their care to someone or somewhere else.

- When their legal status changes (for example, the section of the Mental Health Act which applies to them, or if they are diagnosed with a notifiable disease).

### 2.4 Ensuring that the data subject gives their consent for such use

The data subject must consent to proposed uses of their personal information. They therefore need sufficient information about the potential uses of their information to make an informed choice. Seek advice from the CCG's Caldicott Guardian if in doubt.

If an individual does not consent to a proposed use of their information, then we cannot use it in that way. It is important that an individual fully understands the implications of such a decision and in serious situations where the well-being of the data subject or others may be compromised you should seek advice from the CCG's Caldicott Guardian or IG Lead. Such a decision must be carefully documented and reported to the responsible practitioner.

### 2.5 Ensuring that the data subject understands the limits of confidentiality

You should explain to the data subject that in some limited circumstances you will be obliged to pass on or act upon information even if they object. This will apply if a failure to pass on information may lead to harm to the individual or someone else. There are also certain legal requirements to pass on information that can be explained to the patient if required.

### 2.6 Collecting only what is necessary

You should only collect as much personal information as is necessary for the agreed purpose, and no more. The information collected must be adequate but not excessive. Clearly most healthcare records are by necessity very detailed, but they must nevertheless be accurate and relevant. Where information is extracted for other agreed purposes (for example audit) there should be a sound rationale for every piece of information that is used. Personal identifiers should be removed from the data if they are not strictly necessary for the intended use.

### 2.7 Recording the information accurately

You have a legal obligation to ensure that any personal information you are holding is accurate. Data is regarded as inaccurate if it is incorrect or misleading as to any matter of fact. Data subjects have a legal right to have factual inaccuracies corrected or removed from records, and to have an entry made in their record if they disagree with a statement of opinion.

## 3 Requests for Information on Data Subjects/Service or Staff

- Never give out information on data subjects or staff to persons who do not 'need to know' in order to provide health care and treatment.

- All requests for person identifiable information should be based on a justified need and in some cases may also need to be authorised by the CCG Caldicott Guardian. Any such requests should be passed to the Information Governance

Team who will respond on behalf of the CCG unless it has been formally agreed that the requests will be handled within your Team. See the **CCG Access to Records Policy**.

If you have any concerns about disclosing/sharing person identifiable information you must discuss with a member of the Information Governance Team.

### 3.1 Telephone Enquiries

If a request for information is made by telephone,

- Always check the identity of the caller;
- Check whether they are entitled to the information they are requesting;
- Take a number, verify it independently and call back if necessary.

Remember that even the fact that a patient is in hospital, is a user of the service you work within, or is a member of staff, this is confidential. If in doubt consult your manager.

### 3.2 Requests for Information by the Police and media

**With respect to the Police:**
Requests for information from the Police should always be referred to the Information Governance Manager or the Caldicott Guardian.

**With respect to the Media:**
Do not give out any information under any circumstances. Only trained and authorised Senior Managers are permitted to do so. If you receive any request from the media by personal visit or by phone refer the person to the CCG's Communications, Membership and Engagement Team.

### 3.3 Disclosure of Information to Other Employees of the CCG

Information on patients should only be released on a need-to-know basis.

- Always check the member of staff is who they say they are;
- This can be achieved by checking the employee's ID badge and/or their internal extension number or bleep number prior to giving them any information.
- Check whether they are entitled to the information;
- Don't be bullied into giving out information.

If in doubt, check with the person in charge of the data subjects care or your manager.

### 3.4 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances unless they are directly involved in the patient's clinical care or with the employees' administration on behalf of the CCG. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

If you have concerns about this issue, please discuss with your line manager.

### 3.5 Carelessness

- Do not talk about patients in public places or where you can be overheard;
- Do not leave any health records or confidential information lying around unattended;
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public;
- Always lock your computer screen if you leave it unattended – by pressing the Windows key (bottom left of your keyboard) and the 'L' key together.

## 4 Transfer of Information

**See also CCG Safe Haven Policy**

### 4.1 Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing person identifiable information should always be addressed to a named recipient. This means personal information should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

**Internal** mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

**External** Mail must also observe these rules. Special care should be taken with person identifiable information sent in quantity, such as case notes, or collections of patient records on paper or removable media. These should be sent by Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

**Electronic and removable media** should be encrypted/password protected. Advice on how to password protect files is available via the ICT Team at capccg.ictprojects@nhs.net. **See also CCG Removable Media Policy**

**Case notes** and other bulky material should only be transported in approved boxes and never in dustbin sacks, carrier bags or other containers. These containers should not be left unattended unless stored, waiting for collection, in a secure area e.g. ideally locked. The containers should only be taken and transported by the approved carrier.

### 4.2 Faxing

**Use of Fax Machines banned in the NHS from 1st April 2020**

From **April 2020**, NHS organisations were required to use modern communication methods, such as secure email, to improve patient safety and cyber security. This was part of the Health and Social Care Secretary's tech vision, to modernise the

health service and make it easier for NHS organisations to introduce innovative technologies.

### 4.3 Email

**See CCG Information Security Staff policy**

Please seek advice from your manager or the Information Governance Team if you have the need to email person identifiable information; correct processes must be followed.

**Personal identifiers should be removed** wherever possible, and only the minimum necessary information sent, this may be considered to be the NHS number but no name or address. This in itself can pose problems as the wrong number may have been used. A Data Subject's name should not be included in the subject line of an email; however, initials are permitted.

Special care should be taken to ensure the information is sent only to recipients who have a 'need to know'; always double check you are sending the mail to the correct person(s).

**External transfers** of personal data should only take place to persons with access to a secure account compatible with nhs.net. If a recipient does not have a recognised, secure e-mail account, use of the NHS Mail [Secure] function should be considered. In exceptional cases it may be necessary to email person identifiable information or sensitive or confidential information to persons who only have Internet access. In such cases the potential risk of loss and the insecure nature of using the Internet should be explained and communicated to the intended recipient and their agreement recorded.

## 5 Storage of Confidential Information

Paper-based confidential information should always be kept locked away, preferably in a room that is also locked. In some cases, this may need to be alarmed when unattended, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time.

PC-based information should not be saved onto local hard drives or onto removable media, but onto the CCG's networked 'restricted' drive. Removable media and other media should be kept in locked storage.

## 6 Disposal of Confidential Information

**See CCG Records Management and Lifecycle Policy (Sections on retention periods; destruction and disposal)**

When disposing of **paper-based person-identifiable information** or confidential information always use 'Confidential Waste' bins provided at the CCG base location or by using a cross or micro cut shredder, a strip-cut shredder is not suitable for disposing of confidential personal or patient information. Do not store confidential information where it could be confused with general waste.

**DVD/CDs** containing confidential information must be either reformatted or destroyed. Computer files with confidential information no longer required must be deleted from laptops.

**Note:** DVD/CDs that are no longer required must not be disposed of in the blue confidential waste bins, they must be handed to the CCG's ICT Team or an Egton Engineer.

**Computer hard disks** are disposed of by the CCG's ICT Team or Egton.

## 7 Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone.

- Passwords must not be written down.
- Passwords must not relate to the employee or the system being accessed.

Staff will be given more information about password control and format etc. when receiving their training and/or password.

It is an NHS requirement for encryption to be applied to all CCG devices. To ensure the security of data held on mobile devices including access to NHS Mail accounts, staff must not store their passwords and/or pin numbers alongside any CCG devices issued to them eg a sticker containing a mobile pin code attached to a mobile phone case or writing passwords and pin numbers down in a notebook kept with a laptop or mobile phone.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the Information Governance Manager and may result in a disciplinary action and also to a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 2018, which could lead to criminal action being taken against you.

## 8 Confidentiality whilst Working at Home

**See Working Practices and Standards of Business Etiquette Policy and Procedure**

Please see Section 14 - Confidentiality and Section 15 – Information Governance.

## 9 Copying of software

All computer software used with the CCG is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).

It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach of the license agreement.

## 10 General Provisions

### 10.1 Interpretation

If any person requires an explanation concerning the interpretation or the relevance of this code of conduct, they should discuss the matter with their line manager, a member of the Information Governance team or the Caldicott Guardian.

The CCG's Caldicott Guardian is Carol Anderson, Chief Nurse.

As a consequence of your employment by Cambridgeshire and Peterborough Clinical Commissioning Group, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of the CCG. This condition applies during your relationship with the CCG and after the relationship ceases.

### 10.2 Non-Compliance

Non-compliance with this code of conduct by any person working for the CCG may result in disciplinary action being taken in accordance with the CCG's disciplinary procedure and may lead to dismissal for gross misconduct.

To obtain a copy of the disciplinary procedures please discuss with your manager or the Human Resources department.

### 10.3 Amendments

This code will be amended as necessary to reflect the CCG's development of policies and procedures and the changing needs of the NHS.

## 11 Confidentiality Statement

All CCG e-mails should contain the disclaimer as detailed below.

*This message may contain confidential and privileged information. If you are not the intended recipient, please accept our apologies. Please do not disclose copy or distribute information in this email or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful. Please inform us that this message has gone astray before deleting it. Thank you for your co-operation.*

## 12 Sources of Reference

NHS Digital's Code of Practice on Confidential Information 2018

Cambridgeshire and Peterborough Information Sharing Framework

**Annex A - Equality Impact Assessment Form**

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

## Equality Impact Assessment Form

### Initial Screening

| **Name of Proposal (policy/strategy/function/ service being assessed)** | CCG Code of Conduct for Employees in Respect of Confidentiality Policy |
|---|---|
| Those involved in assessment: | Policy developed in consultation with the IG, BI & IM&T Steering Group and for endorsement by the Integrated Performance and Assurance Committee |
| Is this a new proposal? | No, review and revision of existing policy. |
| Date of Initial Screening: | 31 May 2019 |
| What are the aims, objectives? | The principle behind this Code of Practice is to ensure that employees will not knowingly breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the CCG security systems or controls in order to do so. |
| Who will benefit? | All staff working for and on behalf of the CCG |
| Who are the main stakeholders? | Staff; Managers; IG, BI, IM&T Steering Group |
| What are the desired outcomes? | Staff awarenenss of the Policy through being advised of its availability on the CCG's website via iConnect. |
| What factors could detract from the desired outcomes? | Lack of awareness of the existence of the Policy; Failure by staff to follow the Policy. |
| What factors could contribute to the desired outcomes? | Knowledge of the policy and implementation |
| Who is responsible? | Staff, managers, IG, BI, IM&T Steering Group |
| Have you consulted on the proposal? If so with whom? If not, why not? | Policy developed in consultation with the IG, BI & IM&T Steering Group for approval and endorsement by the Integrated Performance and Assurance Committee. |

| Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick) | | Yes | No |
|---|---|---|---|
| Age | Consider: Elderly, or young people | | X |
| Disability | Consider: Physical, visual, aural impairment, Mental or learning difficulties | | X |
| Gender Reassignment | Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned | | X |
| Marriage and Civil Partnership | Consider: Impact relevant to employment and /or training | | X |
| Pregnancy and maternity | Consider: Pregnancy related matter/illness or maternity leave related mater | | X |
| Race | Consider: Language and cultural factors, include Gypsy and Travellers group | | X |
| Religion and Belief | Consider: Practices of worship, religious or cultural observance, include non-belief | | X |
| Sex /Gender | Consider: Male and Female | | X |
| Sexual Orientation | Consider: Know or perceived orientation | | X |

| **What information and evidence do you have about the groups that you have selected above**? |
|---|
| The above protected characteristics will have no adverse impact as the Policy has been developed in accordance with new Data Protection legislation (ie General Data Protection Regulation May 2018). |

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

| **How might your proposal impact on the groups identified? For example, you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People** |
|---|

Examples of impact re given below:

a) Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc

b) Planning to extend access to contraceptive services in primary care without considering how their services may be accessed by lesbian, gay, bi-sexual and transgender people.

c) Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.

| **Summary** | |
|---|---|
| Positive impacts<br>(note the groups affected) | Negative impacts<br>(note the groups affected) |
| N/A | N/A |

| Summarise the negative impacts for each group: |
|---|
| N/A |

| **What consultation has taken place or is planned with each of the identified groups?** |
|---|
| The Policy was developed and approved in consultation with the IG, BI & IM&T Steering Group prior to endorsement by the Integrated Performance and Assurance Committee. |

| **What was the outcome of the consultation undertaken?** |
|---|
| Approval and Endorsement sought |

| **What changes or actions do you propose to make or take as a result of research and/or consultation?** |
|---|
| Briefly describe the actions then please insert actions to be taken on to the given Improvement Plan template provided.<br><br>The Information Governance Team on behalf of the Associate Director of Corporate Affairs will be responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect. |

| **Will the planned changes to the proposal?** | **Yes** | **No** |
|---|---|---|
| a) Lower the negative impact? | N/A | |
| b) Ensure that the negative impact is legal under anti-discriminatory law? | N/A | |
| c) Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact? | N/A | |

| **Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits**. |
|---|
| Information risk - The CCG must respect patient confidentiality in accordance with the NHS Constitution, ICO Guidance, and the Statutory Code of Practice. 'Necessity' is a qualifying condition to justify the lawful use of PCD. |

| **What monitoring/evaluation/review systems have been put in place?** |
|---|
| Monitoring will be undertaken by the Information Governance team. The frequency of review will be every other year or as required. |

| **When will it be reviewed?** |
|---|
| July 2023 |

| | |
|---|---|
| **Date completed:** | 5th July 2021 |
| **Signature:** | Information Governance Manager |
| **Approved by:** | OD & HR Advisor (Equality and Diversity) |
| **Date approved:** | 15th July 2021 |

## Appendix 1 Glossary of Terms

| | |
|---|---|
| **Patient / Personal identifiable/ Confidential Data (PID/PCD)** | Key identifiable information includes:<br>• a person's name, address, full post code, date of birth;<br>• pictures, photographs, videos, audio tapes or other images of patients;<br>• NHS number and local patient identifiable codes;<br>• 'Online identifiers' include IP addresses and cookie identifiers which may be personal data;<br>• anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified. |
| **Anonymised** | This is information which does not identify an individual directly, and information which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification. |
| **Pseudonymised** | This is like anonymised information in that in the possession of the Information holder it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not. |
| **Clinical Audit** | The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish generalisable knowledge. The first is an essential component of modern healthcare provision, whilst the latter is research and is not encompassed within the definition of clinical audit in this document. |
| **Explicit or Express Consent** | This means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear. |
| **Disclosure** | This is the divulging or provision of access to data. |

| | |
|---|---|
| **Healthcare Purposes** | These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities. |
| **Information Sharing Protocols** | Documented rules and procedures for the disclosure and use of person identifiable information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies. |
| **Medical Purposes** | As defined in the Data Protection Act 2018, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2012 was designed to meet these challenges, by making the NHS more responsive, efficient and accountable. Clinically led commissioning puts clinicians in charge of shaping services, enabling NHS funding to be spent more effectively. |
| **Public Interest** | Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services. |
| **Social Care** | Social care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes “pure” health care (hospitals) and community care (e.g. district nurses) but may include items such as respite care. There is, therefore, no clear demarcation line between health and social care. Social care also covers services provided by others where these are commissioned by CSSRs (Councils with Social Service Responsibilities). |

## Appendix 2 – Professional Codes of Confidentiality

1. **Doctors**

**Extract from General Medical Council**
**'Confidentiality – Good Practice in Handling Patient Information'**

Patients have a right to expect that their personal information will be held in confidence by their doctors. This guidance sets out the principles of confidentiality and respect for patients' privacy that you are expected to understand and follow. This guidance outlines the framework for considering when to disclose patients' personal information and then applies that framework to:

**(a)** disclosures to support the direct care of an individual patient;
**(b)** disclosures for the protection of patients and others
**(c)** disclosures for all other purposes.

This guidance also sets out the responsibilities of all doctors for managing and protecting patient information. In this guidance, we use the terms 'you must' and 'you should' in the following ways.

**(a)** 'You must' is used for an overriding duty or principle.
**(b)** 'You should' is used when we are providing an explanation of how you will meet the overriding duty.
**(c)** 'You should' is also used where the duty or principle will not apply in all situations or circumstances, or where there are factors outside your control that affect whether or how you can follow the guidance.

You must use your judgement to apply the principles in this guidance to the situations you face as a doctor, whether or not you hold a licence to practise and whether or not you routinely see patients. If in doubt, you should seek the advice of an experienced colleague, a Caldicott or data guardian or equivalent, your defence body or professional association, or seek independent legal advice.

You must be prepared to explain and justify your decisions and actions. Serious or persistent failure to follow this guidance will put your registration at risk.

2. **Nurses and Midwives**

**Extract from Nursing and Midwifery Council 'The Code: Professional standards of practice and behaviour for nurses, midwives and nursing associates'**

As a nurse or midwife, you owe a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and that information about them is shared appropriately.

To achieve this, you must:
- respect a person's right to privacy in all aspects of their care;
- make sure that people are informed about how and why information is used and shared by those who will be providing care;
- respect that a person's right to privacy and confidentiality continues after they have died;

- share necessary information with other healthcare professionals and agencies only when the interests of patient safety and public protection override the need for confidentiality, and
- share with people, their families and their carers, as far as the law allows, the information they want or need to know about their health, care and ongoing treatment sensitively and in a way they can understand.

3. **Social Workers**

**Extract from ‘British Association of Social Workers ‘Code of Ethics: Privacy, confidentiality and records’**

Social workers will:

- Respect service users' rights to a relationship of trust, to privacy, reliability and confidentiality and to the responsible use of information obtained from or about them;
- Observe the principle that information given for one purpose may not be used for a different purpose without the permission of the informant;
- Consult service users about their preferences in respect of the use of information relating to them;
- Divulge confidential information only with the consent of the service user or informant, except where there is clear evidence of serious risk to the service user, worker, other persons or the community, or in other circumstances judged exceptional on the basis of professional consideration and consultation, limiting any such breach of confidence to the needs of the situation at the time;
- Offer counselling as appropriate throughout the process of a service user's access to records;
- Ensure, so far as it is in their power, that records, whether manual or electronic, are stored securely, are protected from unauthorised access, and are not transferred, manually or electronically, to locations where access may not be satisfactorily controlled;
- Record information impartially and accurately, recording only relevant matters and specifying the source of information.
- The sharing of records across agencies and professions, and within a multi-purpose agency, is subject to ethical requirements in respect of privacy and confidentiality. Service users have a right of access to all information recorded about them, subject only to the preservation of other persons' rights to privacy and confidentiality.

**Appendix 3 – Relevant Acts of Parliament and NHS Guidelines and what they mean for Employees**

| Requirement | What it covers | Personal responsibilities | Penalties for breaches |
|---|---|---|---|
| Data Protection Act 2018 | Person identifiable information about living individuals – manual and automated records (e.g. on computer, video tape, digital images) | Keep all person identifiable information secure and confidential – see Code of Conduct for specific details | Unauthorised disclosure of personal identifiable information could lead to court action and a criminal conviction and/or the payment of compensation to a claimant. |
| Human Rights Act 1998 (Article 8) | An individual's right to privacy for themselves and their family members | As above | As above |
| Computer Misuse Act 1990 | Unauthorised access to computer held programs and information/data | Do not use any other person's access rights (e.g. user id and password) to access a computer database | A criminal record and a prison sentence of up to 5 years |
| Common Law of Confidentiality | An individual's right to confidentiality of their information when alive and once they have died | Keep all information secure and confidential. Also remember this covers the wishes of deceased persons – if it is recorded that they do not want details of their treatment disclosed when they die this wish will normally need to be respected | Disciplinary action and possible dismissal |
| Caldicott | Security and confidentiality of personal health and social care information for patients and service users | See Code of Conduct – further information available from CCG Caldicott Guardian or Information Governance Manager | Disciplinary action and possible dismissal |
| Contract of Employment | Employees' responsibilities including security and confidentiality of any information accessed during the course of work | Comply with contract and Code of Conduct | Disciplinary action and possible dismissal |