NHS
Rotherham
Clinical Commissioning Group

Title:	**Confidentiality Code of Conduct**
Reference No:	011-IT
Owner:	Deputy Chief Officer
Author	IG Team eMBED Health Consortium
First Issued On:	
Latest Issue Date:	XXX 2017
Operational Date:	March 2017
Review Date:	March 2019
Consultation Process	
Ratified and approved by:	AQuA January 2016 Governing Body February 2016
Distribution:	All staff and GP members of the CCG.
Compliance:	Mandatory for all permanent and temporary employees of NHS Rotherham CCG.
Equality & Diversity Statement:	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination**,** promote equality of opportunity**,** and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

NHS Rotherham Clinical Commissioning Group

NHS ROTHERHAM CLINICAL COMMISSIONING GROUP

Confidentiality Code of Conduct

Version: 2.1

Date: January 2017

Author: IG Team eMBED

Approvals

This document requires the following approvals.

Name	Signature	Title	Date of Issue	Version
			2013	1.0

Revision History

Date of this revision: October 2015
Date of Next revision: October 2016

Revision date	Previous revision date	Summary of Changes	Version
May 2014	N/A	Historic policy updated to reflect up to date current best practice	1.0
August 2015	May 2014	Annual review – edits to the format to make the policy more user friendly and reflect new duties regarding information sharing where appropriate	2.0
January 2017	August 2015	Annual review – minor amendments. Updated YCHS to eMBED throughout Clarified roles of SIRO and Caldicott Guardian Updated sub-AQuA to IG Group	2.1

Contents

NHS ROTHERHAM CLINICAL COMMISSIONING GROUP

Confidentiality Code of Conduct

1. Introduction

In the operation of the organisation, commissioning and the delivery of effective care, NHS Rotherham Clinical Commissioning Group (the CCG) obtains, holds, uses and discloses confidential information. This confidential information may be:

- Information about named individuals (including service users, carers, members of staff and other third parties)
- Information about the CCG, other health or social care organisations or contractors (such as records relating to finance, risk, tenders, contracts etc.)

Keeping information confidential is not the same as keeping it secret. It is essential that relevant and proportionate confidential information is available to those who have a need to know it in order to do their work. Balancing the need to keep information confidential with appropriate sharing may not always be straightforward and advice should be sought from the Information Governance Lead, Caldicott Guardian or Senior Information Risk Owner (SIRO) where there is any doubt. Changes in legislation, the reconfiguration of the NHS and the diversity of service provision in the modern health care system involving close working relationships across different professional groups and health and non-health care agencies, may make it harder to understand what information it is permissible to share and in what circumstances.

This code of conduct is intended to enable the CCG and its staff (including non-CCG staff with access to CCG information) to work effectively in a confidential manner for the benefit of the population of Rotherham and other users of our services. It should help protect patients/service users and staff from the misuse of their information and ensure that confidential information is handled in a lawful and appropriate manner by:

- Defining what is meant by the phrase “confidential information”
- Informing staff of their responsibilities in relation to such information
- Informing staff of the correct procedures for dealing with confidential information so that they do not inadvertently breach confidentiality
- Providing sources of further information

Staff should ensure they are familiar with the content of this Code of Conduct. In particular, they should read section 4, which outlines the principles and requirements of confidentiality that are most likely to be relevant.

If you have any questions about the code you should contact your line manager in the first instance or the Information Governance Lead.

2. Compliance with the Code of Conduct

This code of conduct applies to all NHS Rotherham CCG employees and non-CCG employees who work within NHS Rotherham CCG or under contract to it. This includes, but is not limited to, staff on secondment to the CCG, students on placement, eMBED Health Consortium staff, and people working in a voluntary capacity. For convenience, the term ‘staff’ is used in this document to refer to all those to whom the code of conduct applies.

All staff are expected to comply with this code of conduct and should be aware that any access made to electronic records is auditable and that audits are run periodically on all systems to check that any access made to records is legitimate and required as part of a patient's healthcare pathway.

Any breaches of this code including unauthorised breaches of confidentiality, inappropriate use of personal health or staff records or abuse of computer systems will be treated as a disciplinary offence, which may result in your employment, or association, with the CCG being terminated. It may also bring into question your professional registration and possibly result in legal proceedings. This will also be the case for breaches of commercial confidentiality.

All staff are personally liable for breaches of the Data Protection Act and can be prosecuted in addition to the organisation itself being fined by the Information Commissioners Office.

If the information you are looking for is not covered in this Code you should contact your line manager or the Information Governance Lead for advice. Many of the information governance issues are interlinked so it is difficult to provide information about one topic in isolation.

3. Responsibilities of Staff and the CCG

Caldicott Guardian
The Caldicott Guardian is responsible for approving uses of patient identifiable information. They are a Governing Body level lead who acts as the conscience of the organisation in relation to the use of patient data. Their role is to ensure the organisation processes personal confidential data lawfully and ethically. The Chief Nurse is the Caldicott Guardian for NHS Rotherham CCG.

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner (SIRO) is a Governing Body level person who has overall responsibility for ensuring the organisation handles all personal and organisational information appropriately and lawfully and that processes are in place to manage information risk. The Deputy Chief Officer is the SIRO for NHS Rotherham CCG.

Information Asset Owners (IAO)
CCG information assets must be assigned an Information Asset Owner (IAO). It is the responsibility of the IAO to ensure the assets under their control are protected from unauthorised access and a risk assessment is carried out at least annually.

Managers
All managers are responsible for ensuring that the staff they manage are aware of this Code of Conduct and their individual responsibility for complying with it. They should ensure their staff are equipped to fulfil those responsibilities; this will include by covering it at local induction and by identifying and meeting specific and generic training needs through personal development plans. Senior managers should ensure that managers within their Service area are aware of their responsibilities in relation to staff awareness.

Managers should ensure **ALL** new staff have signed the Confidentiality and Information Security declaration. Managers are required to countersign this declaration to indicate that they have checked that the member of staff has read the relevant information governance policies and has had an opportunity to ask questions about anything they do not understand.

All Staff

All staff must ensure that they are aware of the requirements and standards of behaviour that apply and comply.

All staff are responsible for reporting information incidents and near misses including breaches of confidentiality and information security in line with the CCG's Incident and Near Miss Reporting Policy Incorporating Serious Untoward Incident Procedure. The CCG's incident reporting process is available on the CCG intranet.

The IG Group is responsible for overseeing the implementation of this Code of Conduct including monitoring compliance. It is responsible for ensuring it is reviewed every two years or in line with new guidance or legislation.

Contact details of key IG contacts (for example, the Caldicott Guardian and SIRO) will be made available on the CCG intranet.

4. Code of Conduct

4.1 Confidentiality

4.1.1 What is confidential information?

Personal information is data from which a living individual could be identified; this may include information such as name, age address and personal circumstances. Some personal information is classed as **sensitive personal information** where it relates to an individual's race, health condition, sexuality etc.

Confidential information may also be organisational "corporate" information about the CCG or any other health or social care organisation or external third party.

Within the NHS, person identifiable information about deceased people is recognised as confidential in the NHS Confidentiality Code of Practice, NHS contracts and professional codes of conduct. The duty of confidentiality extends beyond death.

Confidential information may be in a variety of forms including but not limited to electronic, paper, digital or audio format, such as records, note books, message books, x-rays, photographs, audio tapes, voicemail etc., or it may be knowledge gained from overheard conversations or seeing someone sitting in a clinic waiting room.

Examples of confidential information the CCG holds include:

- Personal demographic details of staff (and patients/service users)
- Contact details of staff (and patients/service users)
- Medical details of staff (and patients/service users)
- Ethnicity of staff (and patients/service users)
- Bank and salary details of staff and financial details of service users
- Results of Criminal Records Bureau/Disclosure and Barring Service checks
- Organisational financial information
- Information that is defined as commercial in confidence under the Freedom of Information Act 2000 following a public interest test under Section 43 of the Act
- Information in relation to concerns and complaints

Information that has been placed in the public domain, except as a result of a breach of confidentiality, is not classed as confidential.

4.1.2 Who has a duty of confidentiality?

All CCG employees and non-CCG employees who work within NHS Rotherham CCG or under contract to it have a duty to maintain the confidentiality of information gained during their employment/association with the CCG. This includes, but is not limited to, eMBED Health Consortium staff, staff on secondment to the CCG, students on placement and people who are working in a voluntary capacity. For convenience, the term 'staff' is used in this document to refer to all those to whom the code of conduct applies.

Anyone may come into contact with confidential information in the course of their duties. For example:

- You may have direct access to confidential information if you are authorised to access information held in: staff or patient/service user records; records about complaints, incidents, safeguarding; a register of concerns; contracts and etc.
- You may have confidential information passed to you in connection with your work
- You may become aware of information as a result of breaches of confidentiality

You are obliged to maintain the confidentiality of this information under the Data Protection Act 1998, Computer Misuse Act 1990, Caldicott guidance and NHS contractual obligations. Unless the information places a person at significant risk of harm, then staff have a duty to co-operate to protect the individual or public. This duty continues after you no longer work for/have an association with NHS Rotherham CCG.

4.1.3 Why is confidentiality important?

Confidentiality is important to protect the privacy of all individuals (staff and patients), and the commercial confidences of third parties, whose information we hold, to enable NHS Rotherham CCG and its partners to conduct their business effectively.

Both staff and service users provide NHS Rotherham CCG with confidential information about themselves in the course of the CCG's business activities. They have a legitimate expectation that we will respect their privacy and treat their information appropriately.

As part of the wider NHS and in delivering its own services, it is important that NHS Rotherham CCG maintains the trust of patients. Patients/service users entrust health services with, or allow us to gather, confidential information relating to their health and other matters as a part of their seeking treatment/accessing services. We use this information to assess their needs and deliver appropriate treatment and care; including an audit of such care. We also use this information in a pseudonymised form for secondary purposes such as the planning and management of services.

It is essential that clinicians/practitioners have all relevant information to hand when treating or caring for people. If patients/service users do not trust us with their information they may withhold vital information or not seek treatment. In addition, services may be planned on the basis of inaccurate information about the health needs of the population.

In some circumstances, service users may lack the competence to extend their trust or may be unconscious, but this does not diminish the duty of confidence.

Trust is important in managing health and safety, and risk. Staff or patients may want to pass on information about other individuals, for example, to report poor practice, incidents or near misses. Staff should be aware of the appropriate procedures, which should be followed in such cases.

The CCG works in partnership with partner organisations and third parties in order to discharge its duties. Lack of confidence in the CCG to maintain confidentiality would seriously impede the CCGs abilities to operate effectively. This does not affect NHS Rotherham CCG's commitment to work in an open and transparent manner under the principles of the Freedom of Information Act and other legislation and to disclose information where it is lawful to do so.

It is essential if the trust of staff and patients/service users is to be retained, and legal requirements are to be met, that the NHS provides, and is seen to provide, a confidential service.

4.2 Staff Responsibilities

4.2.1 Inform patients/service users/staff about how we use their information

Being open and transparent with people about who you are, what your role is, why you are collecting information, how you will use it, who you may share it with and gaining consent is not only integral to processing information fairly under the Data Protection Act but is at the heart of addressing many issues around information sharing and confidentiality.

At a patient/service user/member of staff's **first contact** with the organisation /service/ event (such as an investigation) or at the most appropriate time thereafter:

DO…

- Explain to the patient/service user/carer/member of staff: why we collect information, how it might be used, who it might be shared with and seek their consent.
- Remember that information required to facilitate the provision of direct care can be shared between health and social care professionals in the best interests of their patients within the framework set out by the Caldicott principles.
- Make it clear to individuals what your role is and the circumstances under which confidential information may have to be shared. This gives them the opportunity to make an informed choice as to what information they disclose to us.
- Explain to patients/service users in particular that the information they give may be recorded, may need to be shared in order to provide them with optimal care and may be used to support clinical audit, service evaluation and other work to monitor the quality of care provided.
- Explain to individuals their general rights (see section 4.3).
- Consider if individuals would be surprised to learn that their information is being used in a particular way. If they would be surprised, they are not being effectively informed and this may lead to mistrust in the professional and the organisation.
- Ensure that there is a **legal basis** where any personal information is used or considered for use by the organisation.

DO NOT…

Disclose or use information that can identify individual patients for any purpose other than direct healthcare **UNLESS**:

- The individual patient or patients have given their explicit consent for the information to be disclosed or used for specific purposes
- There is a legal obligation to disclose the information (e.g. Court Order)
- There is an overriding public interest to disclose the information e.g. to safeguard an individual, assisting a serious crime investigation.

CONSIDER…

- Has the patient/service user been provided with a generic information leaflet or a service specific information leaflet?
- Has the patient/service user had the opportunity to read the leaflet and ask questions?
- Is it clear to the patient/service user when information is recorded or health records accessed?
- Is it clear to the patient/service user when staff are already or will be sharing information with others?
- Is the patient/service user aware of the choices available to them in respect of how their information may be used or shared?
- Have you checked that the patient/service user has no concerns or queries about how their information is used or shared?
- Does the patient/service user have a learning disability, alternative communication needs, capacity issues that requires additional or specialist support in order to engage with them as fully as possible?
- Answer any queries personally or direct the patient/service user to others who can answer their questions or to other sources of information. The Information Governance Team at eMBED Health Consortium can also be contacted.
- Respect the rights of patients/service users and facilitate them in exercising their right to have access to information in their health records.

4.2.2 Records Management – creation and disposal

DO…

- Record information accurately, consistently and in a timely manner
- Record information in accordance with CCG policy and service specific procedures (see the Records Management Policy and any local procedures relevant to your work area).
- Maintain accurate records. (This is vital to the provision of services and the running of the CCG.) If records are inaccurate, future decisions may be wrong and may result in harm to a service user or member of staff, and/or an inefficient or ineffective use of resources.
- Be consistent. If information is recorded inconsistently, it will be harder to interpret which may result in delays and possible errors or a lack of accountability.
- Dispose of confidential waste appropriately and in line with CCG policy - confidential information may be stored in a number of formats (including removable media and hard drives of smartphones/computers etc)

4.2.3 Use confidential information in accordance with NHS Rotherham CCG policies

DO…

- Be aware of all relevant CCG policies and procedures. An up to date list is available on the intranet. Contact the Information Governance Lead for clarification of anything you do not understand.
- Be aware of the issues surrounding confidentiality, and seek training, support and advice as necessary in order to deal with them effectively.
- Feedback comments or suggestions to managers on systems, procedures or working practices that give a cause for concern or could be improved.
- Inform the staff you manage (or sponsor) what their responsibilities are in relation to information governance policies and what this means for them in their day to day work;
- Ensure that service/team specific procedures are in place to implement CCG policy where required.
- Ensure staff are appropriately trained in information governance relevant to their role.
- Ensure information governance policy and process is adhered to and action taken to address non-compliance.
- When staff leave, inform relevant people within the CCG so that their IT accounts/access to information systems can be disabled, ensure security passes, USB sticks, laptops, mobile phones etc. are returned.
- Report breaches, suspected IG breaches and near misses (see s.4.2.4)

DO NOT…

- Attempt to prove a suspected security weakness, as testing a weakness might be interpreted as a potential misuse of the system
- Allow third parties access to the CCG's hardware and equipment, without correct authorisation
- Be afraid to challenge anyone who you were not aware would be in the organisation
- Ignore security incidents

4.2.4 Incident Reporting

Information governance incidents, including near misses, should be reported in line with CCG policy. Information incidents include but are not limited to: lost records or other information losses (for example, confidential personal or organisational information, business critical information), breaches of confidentiality, breaches of security, loss of IT equipment, cyber security incidents, inaccurate record keeping, sharing of passwords or smartcards, inappropriate use of information.

The use of or disclosure of information without a legal basis is a breach of data protection principles and as such should be reported as an Information Governance incident in line with CCG policy.

4.2.5 Use of Social Networking media

Social computing includes but is not limited to: blogs, online discussion forums, collaborative spaces, media sharing services and microblogs. Examples are Blogger, JISC mail, facebook and twitter. This media is widely used and has many benefits. However, it is easy to inadvertently use it inappropriately.

The communication is informal and with the many connections that are made between people it is easy to blur the boundary between work and personal life. As an informal method of communication it is easy to publish content that you may later regret and which may not be appropriate in a work context. Such information may end up having a much wider audience than you anticipated which cannot later be retracted.

DO…

- Be aware that failure to adhere to the CCG's Internet Acceptable Use Policy may result in being subject to disciplinary procedures.
- Take care to use social computing media, whether for work purposes or personal use, in a manner that is consistent with the terms and conditions of your employment or association with the CCG.
- Obtain prior approval before using social networking or blogging media at work when representing the CCG in an official capacity and use social media in a professional manner
- Think carefully about what you publish even outside of work - inappropriate use could lead to disciplinary action
- Where appropriate, you should identify that any views expressed are your own and not those of your employer

DO NOT…

- Post content that breaches confidentiality, contains inappropriate comments about colleagues, service users, members of the public, is abusive or hateful, or would potentially cause embarrassment or detrimentally affect the reputation of the CCG.

4.3 Patient/Service User/Staff rights

4.3.1 Rights of individuals in relation to their information (including the right to access personal information) (see also sections 4.4 and 4.5)

Under the Data Protection Act, individuals (known as data subjects) have certain rights about the way information about them is used. These include:

- The right to request access to information that is recorded about them (a subject access request) and to be provided a copy of that information with an explanation of any part of it they do not understand. (Data subjects can authorise a third party to request access on their behalf.)
- The right to prevent the processing of information causing unwarranted damage and distress.
- The right to have inaccurate information rectified or destroyed. (In cases of dispute, the individual will be allowed to place a note on the record disputing the CCG's version of events.)
- The right to seek compensation.

Children and young people have a right to see information about them if they are 'Gillick/Fraser' competent (where for children under the age of 16 years parental rights yield to the child's right to make his/her own decisions when he/she reaches a sufficient understanding and intelligence to enable him/her to understand fully what is proposed).

People with parental responsibility can apply to see a child/young person's records but this will be refused if a child is Gillick/Fraser competent and does not consent.

4.4 Consent

4.4.1 Consent to obtain information

See section 4.2.1: Inform patients/service users/staff about how we use their information and seek consent. Information collected for one purpose may not be used for another, incompatible, purpose without consent.

4.4.2 Consent to use/share personal information

DO…

- If personal information is to be used or shared, **wherever possible**, obtain the **informed explicit consent** of the individual to whom it relates. Informed consent is when an individual understands why their information is needed, how it will be used, who it will be shared with, the possible consequences of them agreeing or not to that proposed use, and gives consent. Consent may be explicit or implied, depending on the circumstances. (Ask the IG Lead for advice.) Explicit consent may be given orally or in writing.
- Where a third party (such as a solicitor or family member) requests access to records and has provided written consent of the individual, check with the data subject that the consent is informed.
- Inform patients/service users/staff that they generally have a right to object to the use and disclosure of confidential information that identifies them. In certain circumstances, if a patient/service user chooses to prohibit the disclosure of information to other relevant professionals it may mean that the service that can be provided is limited or, in rare circumstances, cannot be provided at all.
- Inform patients/service users/staff if their decisions about disclosure have implications for the provision of a service.
- Even where there are grounds for sharing information without consent it is good practice to ask permission to share that information (unless it would prejudice the investigation of a crime or would put the individual at risk of harm).

Where a patient/service user has been informed about the proposed uses and disclosures involved in the delivery of a service and their right to refuse permission, and they agree to their information being shared, then explicit consent is not required for each specific disclosure associated with that service. For example, the sharing of information within a multi-disciplinary team does not require explicit consent for each disclosure.

Lack of consent should not prevent the sharing of information where there are concerns about the welfare of an individual. Disclosures without consent should only be done with appropriate authorisation (see section 4.4.3).

4.4.3 Consent: Capacity to consent (see also 4.3 and 4.5.1)

Where an individual does not have the capacity to consent, the responsibility for deciding the appropriate course of action lies with the agency giving care or, for patients/service users who have planned ahead, the person with lasting power of attorney (LPA).

Where the agency giving care is responsible for decisions about information sharing, these must be made in the best interests of the patient/service user taking into consideration any previously expressed views of the client.

In accordance with the Mental Capacity Act 2005 (MCA), the agency, where appropriate, should consult other people, especially: anyone previously named by the patient as someone who should be consulted, carers, close relatives or friends of the patient, any attorney appointed under the MCA, the views of an appointed independent mental capacity advocate (IMCA), any deputy appointed by the Court of Protection to make decisions for the patient.

4.4.4 Consent: Children and young people (see also 4.3 and 4.5.1)

Young people of 16 years and older are presumed to be competent to give their own consent. Children who are 16 and over but lack capacity to make decisions, follow the same path as adults who lack capacity (see 4.4.3) but they cannot make an advanced decision until the age of 18 nor can they apply for a LPA until the age of 18.

In the case of children and young people under the age of 16, consent is usually required from one person with parental responsibility (who is usually the mother or father or someone who holds a court order giving them parental responsibility).

As children get older they gain rights for themselves. Children under the age of 16 can give consent for themselves if they have sufficient understanding and intelligence to fully understand what is proposed, that is, they are Gillick/Fraser competent (see section 5.3).

People with parental responsibility can authorise other people to make decisions about their children including the sharing of information.

4.5 Disclosing personal information

4.5.1 Subject Access Requests (including access to the health records of deceased people) (see also 4.4 and 4.5.5)

The 1998 Data Protection Act governs the personal information of living individuals (known as data subjects). Data subjects have a general right of access to **view or receive a copy of information** that is held about them. An individual can apply for access to his/her own information or authorise someone else to apply for access to this information on his/her behalf (known as a subject access request).

DO…

- Refer to the CCG's Data Protection and Subject Access Request policy
- Ensure that subject access requests and requests for access to a deceased person's record are made in writing
- Verify the identity of the requester
- Respond to requests within 40 calendar days for Subject Access Requests and 21 days for Access to a Deceased Person's Records request (the requester must provide sufficient information in order for the CCG to be able to locate the information. The clock stops until this information is provided and the fee, if requested, has been paid.
- Ensure explanations are provided to data subjects of any information they do not understand (explanations of abbreviations etc.)

- Ensure that the records are checked and that any information which may cause serious harm to the health of the data subject or anyone else is redacted prior to release of the records.
- Ensure that any information within the records that identifies another person (unless they have consented to the release of the information) is redacted prior to release of the records. Consent to release information provided by a third party is not required if the third party is a health professional involved in the care of the individual unless and the information concerned relates to the individual's care
- For requests to access the health records of deceased people, these can be made under the Access to Health Records Act 1990. Under this Act, the patient's personal representative or anyone with a claim on the deceased's estate can request access to their records. Only information relevant to the claim should be released. Advice should be sought from the Information Governance Lead. Decisions to disclose or withhold information should be made on a case by case basis.

4.5.2 Disclosing information without consent (see also 4.5.3, 4.5.4 and 4.5.5)

There are circumstances when it is necessary to share information even though the individual has not consented. These circumstances are the **exception** rather than the rule.

Information **can be shared without the consent** of the person whom the information is about when:

- It is in the public interest to do so
- It is required by law
- It is required to facilitate the **provision of direct care** between health and social care professionals who have a legitimate relationship with the person as long as the person is unlikely to object (where the whole record is required to be shared, this should only be done on the explicit consent of the individual)

Examples of sharing information in the public interest include:

- Where a child is believed to be at risk of harm (Children Act 1989).
- Where there is a risk of harm to anyone including the data subject.
- Where information is required for the prevention, detection or prosecution of a crime.
- Under the Mental Health Act 1983 where a service user objects to their 'nearest relative' being consulted re:
  - An application for Treatment Order (Section 3) is being considered
  - An application for assessment and/or treatment in relation to the service user has been made.
  - Under the Mental Health Act (Patients in the Community) Act 1995 where the service user is known to have the propensity to violent or dangerous behaviour.
- Domestic Violence, Crime and Victims Act 2004 gives victims of specified sexual or violent offences the right to be informed of certain decisions if the offender becomes subject to provisions under the Mental Health Act 1983.

Examples of sharing information where it is required by law include:

- Notification of certain infectious diseases
- Where it is required by court order

Confidential information that is disclosed without consent must follow the appropriate process (see section 4.5.3, 4.5.4 and 4.5.5)

4.5.3 Disclosing information without consent (see also 4.5.1, 4.5.4 and 4.5.5)

The appropriate procedure to follow must be decided on a case by case basis.

DO:

- Decide on a case by case basis whether it is appropriate to disclose information without consent.
- Inform the individual of the decision taken to share information without consent (unless it would prejudice the investigation of a crime or would put the individual at risk of harm). It may be appropriate to give the individual an opportunity to disclose the information him/herself.
- If it is not possible to obtain the consent of the individual, or it is not desirable, then the decision to share information should be taken at an appropriately senior level within the organisation.
- Ask your line manager for the procedure you should follow or obtain advice from the Information Governance Lead
- The authority to disclose information may vary within different parts of the CCG and may depend on the reason for and/or circumstances of disclosure. It may lie with the Caldicott Guardian/SIRO/Information Governance Lead, or professional leads (for example, safeguarding).
- Requests requiring Caldicott approval should, unless there are exceptional circumstances, be routed via the Information Governance Lead where such requests are made by the Police, UK Borders Agency or any other government agency, or where the information is required for research/analysis purposes, unless there are local procedures in place (for example, safeguarding). This is to ensure that all such requests are logged and the reason for decisions recorded centrally.
- Record the reasons for the final decision (either to share or not to share)
- Document what information was released and when, to whom it was disclosed, and why it was felt justified where information is shared without consent.
- Ensure that decisions not to share information are also justified and documented. Staff and/or the CCG can be held accountable for acts of omission as well as commission.
- Report all non-consented disclosures must be reported to the Information Governance Lead for logging unless they are part of a delegated process, for example, Safeguarding Procedures.

4.5.4 Disclosing information to the police (see also 4.5.1, 4.5.2 and 4.5.3)

DO…

- Direct all requests for personal information from the police via the IG lead.
- Ensure requests are made in writing which can include faxes on headed paper and attachments from a personal police email account (i.e. *.pnn.police.uk).
- Verify the identity of the requestor.
- Ensure that the request for information specifies why it is required. (See section 4.5.2 for legitimate reasons for disclosing information without consent.)
- If it is not possible for the applicant to specify why the information is required (for example, because it would prejudice the investigation of a crime) then the request should be signed by a senior officer.
- Only disclose information with the proper authority (See section 4.5.3 and 4.5.5 (iv)).
- Disclosures to the police may be very sensitive. Consider if special arrangements need to be put in place to facilitate disclosure, for example, the nomination of a specific member of staff to deal with the request.
- Where police produce a consent form for the records they wish to access, a CCG member of staff should check with the data subject that the consent is informed. Staff should be mindful of the impact that sensitive information in a patient's record may have on the individual.

4.5.5 Checklist before disclosing confidential information (see also 4.5.1 and 4.5.3)

The purpose of these questions is to help you decide the appropriate action to take if you are asked to disclose confidential information about a patient/member of staff. They are not sequential or definitive but are intended as a guide to good practice.

i) Have I verified the applicant's identity?
ii) Is there a legitimate reason for disclosing the information?
iii) Is the information requested adequate, relevant and not excessive for the purpose?
iv) Do I have the authority to disclose the information?
v) What is the most appropriate method of disclosing the information?
vi) Who do I need to inform that I have disclosed confidential information?
vii) What do I need to record about the request and disclosure/non-disclosure?
viii) Where do I record information about disclosure/non-disclosure?
ix) Do I need to report the disclosure/non-disclosure to anyone?

i) Verifying identity

Requests by the data subject or on behalf of the data subject

Photo identification and verification of address such as a utility bill should be provided.
If the request is made on behalf of a data subject then proof of the relationship (for example, power of attorney, legal representative etc.) should be provided.

Request from another agency (for example, police, local authority)

Telephone requests
Telephone the individual back via the main switchboard of their organisation (in addition, verify with switchboard if the person is employed there in their stated capacity). If you do not know the telephone number (for example, because it is an agency that you are not familiar with), then you should independently verify the number via a telephone directory/directory enquiry service; do not accept the number as given by the applicant.

Unless there is a local procedure in place that states otherwise, you should ask for the request to be put in writing (which includes by fax or email attachment from a secure domain). All requests from the police and other Government agencies should be put in writing.

Written requests
Written requests from organisations (for example, a solicitor or substance misuse agency) must be on headed notepaper. The address should be independently verified (that is, you should not accept an address/fax number given to you for an organisation that you are unfamiliar with). The identity of the applicant should be verified for all written requests.

ii) Legitimate reasons for disclosing information

- The patient/service user/staff member wishes the information to be disclosed.
- Disclosure is required by law, for example, by statute or court order.
- The public interest in disclosing the information overrides the public interest in maintaining confidentiality.
- Disclosure of the information is required for the purposes of providing care.

iii) Disclosing information that is adequate, relevant and not excessive for that purpose

Consider:

- What does the recipient hope to achieve by the disclosure? (That is, what is the purpose of disclosing information?)
- What is the minimum amount of information you can share to achieve that purpose?
- Who does the information need to be shared with?

iv) Authority to disclose information – consented and non-consented disclosures including routine transfers of Personal confidential information (PCD)

Confidential personal or CCG information may only be disclosed with the proper authority and must be protected against improper disclosure at all times. Authority to disclose may be obtained from the patient/service user/staff member or from the designated individual in the CCG.

Authority from the patient/service user/staff member
The patient/service user/staff member has given authorisation for the disclosure of his/her information.

Appropriate authority from within the CCG
Disclosures of information that breach confidentiality should be authorised by the Caldicott Guardian/Senior Information Risk Owner/Information Governance Lead unless part of an authorised process such as safeguarding. (Advice can be obtained from the Information Governance Lead) All non-consented disclosures that fall outside of safeguarding or other local procedures should be reported to the Caldicott Guardian via the Information Governance Lead.

All routine transfers of personal confidential information (PCD) must be authorised by the Information Governance Lead. All services should provide an up to date map of PCD flows to the Information Governance lead so that these flows can be risk assessed. This is a requirement of good information risk management and the Information Governance Toolkit.

v) Appropriate methods of communicating ALL confidential information (including safe haven procedures) (See also 5.5.6)

The most appropriate method of communicating information will depend on a number of factors including the sensitivity of the information, its destination and the urgency of the request. Information should be transferred effectively, that is, it should reach its destination in a timely manner, and securely. As a general rule, safe haven procedures must be followed (see 5.5.6). That is, you should inform the intended recipient that you will be sending them confidential information, you should agree on a secure method of transfer and you should request acknowledgment of its receipt.

By post

- Ensure you have an up to date address for the intended recipient.
- Confidential information should be addressed to a named individual or team and marked *'Private and confidential: for the addressee only'*.
- Confidential information sent in both the internal and external post should be in sealed envelopes or packaging and must include the full postal address.
- Depending on the sensitivity of the information and where it is being sent to, information may be double or single wrapped and delivered by hand/ recorded delivery/ normal post/ internal post. Confidential information must not be transferred in a transit envelope whether it is sealed or unsealed.

- Information sent through the internal post should contain the name of the service and the full work base address.
- Information sent/transferred on portable media such as a DVD, CD rom or USB stick must be encrypted.

By telephone

Ensure you know the identity of the caller before giving out information (see 'verifying identity' above). Do not leave confidential information on voicemail.

By email

Confidential information should not be shared by e-mail unless it is part of a work flow process agreed and authorised by the Information Governance Lead. Only encrypted transfers are permitted. Safe haven procedures should be followed. (See Email policy)

By text

Confidential or sensitive information must not be sent by SMS text message.

By fax

- Personal confidential information should not be sent by fax - only use if a better alternative isn't available.
- Where it is necessary to fax confidential information, it should be faxed to a safe haven fax, where possible, using safe haven procedures.
- A safe haven fax is one that is located in a separate office that has restricted access.
- Confidential information can be sent to faxes situated in open plan offices by using safe haven procedures: The intended recipient should be telephoned and informed that you are about to send them confidential information. The intended recipient should wait by the fax machine and collect the fax immediately it arrives. The recipient should telephone you to let you know it has arrived.
- Always fax information to a named recipient or team.
- Routinely used numbers should be pre-programmed into the fax machine.
- Faxed information going astray is usually down to user error so it is important to take care to enter the fax number accurately. If there is any doubt, a test fax can be sent followed by the confidential fax using the redial button.

All routine flows of patient confidential data should be mapped and a copy given to the Information Governance Lead. It is the responsibility of the Information Asset Owner to ensure that the information flow is mapped and risk assessed at least annually.

vi) Informing appropriate individuals that confidential information has been disclosed

The patient/service user/staff member

1. Even where there are grounds for disclosing confidential information without consent it is good practice to ask permission to do so. However, the patient/service user/staff member should not be asked for permission to release information or told that information about them has been disclosed without their consent if it would prejudice the investigation of a crime or would put any individual at risk of harm. Not asking permission will be an exceptional event.
2. Where a patient/service user/staff member has disclosed information that you feel needs to be disclosed to a third party, it may be appropriate to give the patient/staff member an opportunity to disclose this information him/herself first. You should follow this up later, by an agreed date with the individual, to ensure the information has been disclosed.
3. If it is decided that it is necessary to disclose information even though the patient/service user/staff member has specifically withheld their consent, it is good practice to inform him/her of your intention (unless to do so would prejudice the investigation of a crime/result in harm – see point 1).

Other individuals within the CCG or in other organisations

It is important to identify and inform any individuals who need to be made aware that confidential patient/service user/staff member information has been disclosed. This is particularly important where information has been disclosed without consent.

vii) Recording information about disclosures

All relevant information about disclosures must be recorded in the patient's notes/staff personal file or organisational folder.

This includes:

- The name of the person and agency making the request
- The method of the request (telephone, in writing, by fax etc)
- The purpose of the request
- Whether information was disclosed or not
- Who the information was disclosed to and by what method
- Reasons for disclosure or non-disclosure
- If there was consent to the disclosure or not (include reasons where consent was not obtained)
- Who has been informed of the disclosure

Disclosures that are reported to the Caldicott Guardian/Information Governance Lead are recorded and held in a central log.

4.5.6 Safe Havens and safe haven procedures (see also 5.7 and 5.5.5 (v))

Safe havens and safe haven procedures are associated with the secure transfer of patient information. There are two types: Local Safe Havens and Traditional Safe Havens, both of which are there to protect the security and confidentiality of information:

Local Safe Havens and their associated processes relates to the storage and use of confidential information. A Local Safe Haven incorporates the secure storage of information (for example, in a locked filing cabinet or in an electronically held folder or database where access is restricted and managed by the Information Asset Owner. Local Safe Haven processes enable the CCG to control access to this information and ensure its use is authorised for approved purposes.

Traditional Safe Havens and safe haven procedures refer to the secure transfer of patient identifiable information for operational purposes that are related to the direct health and social care of patients, for example referrals for services. Historically relating to faxed information for invoicing, safe haven procedures should be used when transferring confidential information by whatever method unless there is a documented exception.

DO…

- Use safe haven procedures without exception for all ad hoc transfers. Safe haven procedures include informing the intended recipient that information is going to be transferred, checking the address (email or fax number) of the intended recipient and requesting confirmation that it has been received.

- Contact the intended recipient prior to sending the information to ensure it will be received in a timely manner, for example, to check the recipient is not on leave.
- Check if any proxy access has been given to the account where email is used, and whether it is appropriate to send the information in such circumstances.
- Inform the recipient why the information is being sent and check that the information will be managed appropriately, for example, where email is used, that it will be deleted from the email system.
- Put in place a system for confirming receipt of the information. This may be a direct request for confirmation from the recipient or a 'by exception' process where regular transfers of information are involved. That is, information is sent on a particular date and the intended recipient informs the sender if information is not received when expected. Non-receipt of information should be followed up and reported as incidents.

4.6 Information Security

4.6.1 Use of portable devices

DO…

- Use portable devices in line with CCG Policy.
- Use only portable devices that have been provided by or authorised for use by the IT Department for work purposes. This includes, but is not limited to, laptops, tablets (for example, ipads), USB sticks, digital dictation machines and smart phones.
- Ensure all portable devices are protected by appropriate security. Portable devices such as laptops, tablets (for example, ipads), dictation machines smart phones and USB sticks **must** be encrypted and, where appropriate, have up to date anti-virus software.
- Ensure confidential information held on a portable storage device such as a CD/DVD is encrypted
- Portable devices used to access NHS mail must be encrypted and have the capacity, and be configured, to allow remote wiping.
- Ensure portable storage devices (including CDs, DVDs and flash drives) containing software or data from external sources, or that have been used in external equipment, are fully virus checked before being used on CCG equipment and are protected by proper security (ask IT Service Desk for advice).
- Obtain authorisation for working on confidential information from home (see section 4.6.3)
- Only use portable devices to transport confidential or sensitive information when other more secure methods are not available.
- Ensure all information, confidential or otherwise, is transferred using encrypted portable media.
- Always transfer information back to its normal storage area as soon as possible. Failure to do this may result in problems with the version control or the loss of information if the portable device is lost or corrupted.
- Always remove information from portable media after it is no longer needed.
- Contact IT Service Desk as soon as possible in the event of loss, theft or damage to your portable device.
- Ensure that any suspected or actual breaches of security are reported via the CCG incident reporting procedures and to the Information Governance Lead directly or via the IT Service Desk.

DO NOT…

- Hold confidential information on portable/mobile devices such as laptops, ipads, memory sticks, mobile phones or PDAs without the prior approval of line management and, where appropriate, the SIRO. It must not be held on personal portable devices.
- Use personal USB sticks on work equipment.

- Use portable devices as storage devices. This media is a means for transferring data and is not intended to be used for long-term storage nor is it an adequate back up device. The CCG's network provides all users with the facilities to save information securely in folders that are backed-up on a daily basis. CDs and DVDs may be used to store information where this is part of the organisational record subject to compliance with CCG Information Governance requirements – contact the IG Lead for advice.
- Leave portable equipment in places vulnerable to theft.
- Leave portable equipment visible in a car; always lock it away in the boot.
- Install unauthorised software or download software from the internet without authorisation from IT.
- Connect personally owned devices directly to the CCG network. Directly connected means either by wire (network cable) or wifi. The network means the library and personal drives on the server or intranet. Personally owned means devices that are not provided by the CCG. (Procedures are in place for connecting the devices of staff who work for 3rd party organisations – Ask the IT Service Desk) Devices include home personal computers, laptops, notebooks (for example, ipads), media players (such as iPods) and smart phones. An exception is PDAs, which may be connected to your PC via a USB port in order to synchronise diaries. This requires prior authorisation of the IT Service Desk.

4.6.2 Security (see also 4.5.5 (v) and 4.7)

Personal information should be held, used and shared securely and confidentially and in line with CCG policies and procedures including the Information Security Policy. See guidance below:

i) Confidentiality in public places

DO…

- Be aware of the difficulties of maintaining confidentiality in open plan offices.

DO NOT…

- Do not discuss confidential information in public areas where it may be overheard, for example in corridors, in reception area, when using mobile phones
- Record confidential information where it may be accessed by unauthorised people – for example, on post it notes, systems that are not protected by proper security, notice boards, card systems that are not locked away etc.
- Work on confidential information in public places such as trains or coffee shops.

ii) Access to information

DO…

- Save all information (confidential and non-confidential) on a secure server where available.
- Ensure confidential information stored in a shared drive is accessible only to those with a need to know.
- Consider how PC screens are positioned. Can confidential information be seen by anyone who does not have a need to know?

- **Lock your work station** even when you are away from your desk for short periods such as to make a cup of tea or take a comfort break (use windows 'L').
- Share information on a need to know basis.

DO NOT…

- Browse electronic systems or records.
- Access information which you do not have a need to know.
- Leave confidential information unattended, for example, do not leave information out on your desk or leave your desk when you are logged onto information systems.

iii) Information Security

DO…

- Lock information away when not in use.
- Ensure information not stored on a server, for example, information held on a PC or laptop hard drive is encrypted and backed up regularly, kept in a secure place and transferred to a server at the earliest opportunity.
- Use up to date anti-virus software.
- Virus check flash drives before introducing them onto your PC.

DO NOT…

- Use portable devices should to store person identifiable data without prior notification to the Information Governance lead in accordance with CCG policy (see section 4.6.1)
- Introduce unauthorised software onto your PC or laptop.

iv) Send personal information appropriately (see 4.5.5(v))

DO…

- By post – to a named person or team in a sealed envelope marked 'Private and confidential: for the addressee only'
- By portable media – information must be encrypted and transferred appropriately
- By telephone – ensure you know the identity of the caller before disclosing information (See 4.5.5(i))
- By E-mail – confidential information should not be shared by e-mail unless it is part of an authorised process (see Email Policy)
- By text – SMS may be used to contact patients/clients, for example, to remind them of appointments. Texting should only be done with the consent of the individual concerned. The Information Governance Lead must be contacted prior to setting up such a system.
- By fax – to a named person or team, include your contact details, use safe haven procedures, for example, telephone the recipient before faxing to ensure they are there to collect it (Consider if there it is appropriate to send information by fax - only use if a better alternative isn't available.)

DO NOT…

- Leave confidential messages on voicemail
- Send personal information by SMS text message.

v) Passwords

DO…

- Use passwords to access electronic systems in line with CCG policy, for example, in deciding what the password should be, how often it is changed, not sharing passwords, locking workstations, password protecting documents etc.
- Change your password at regular intervals
- Avoid using short passwords or using names or words that are associated with you, for example, children's or pet's names
- Use a combination of numbers, letters (upper and lower case) and characters

DO NOT…

- Share passwords or smartcards with others
- Re-use old passwords
- Write your passwords down in a way that would allow another to access it/use it to access your account
- Allow others to use your smart card or share the pin number with anyone

4.6.3 Working from home (see also 4.6.1 and 4.6.2)

DO…

- Only work from home in accordance with the CCG policy around home working, remote working and the use of portable devices
- Staff who regularly work from home should request access to the CCG network which will remove the need to use USB sticks etc.

DO NOT…

- Place confidential CCG information on personal equipment such as PCs, laptops, USB sticks, DVDs
- Place confidential information on CCG provided portable media such as USB sticks and DVDs unless they are encrypted and the use has been authorised by line management.

4.7 Using data for secondary uses

4.7.1 Rules regarding the use of patient identifiable information for non-direct care (secondary purposes) (see also 4.5.6)

The Health and Social Care Act 2012 introduced new restrictions on secondary use of identifiable data.

DO…

- Only use person identifiable data for purposes not involving direct health care (that is, for secondary purposes) where there is a legal reason to do so. Legal reasons include patient consent or approval from the under section 251 of the NHS Act 2006.
- If you are currently using patient identifiable data for secondary purposes, or you think you need to use patient data for non-direct care work, you must contact the Information Governance Lead for advice on what is permissible.

4.8 Freedom of Information Act, Environmental Information Regulations and requests for information

Under the Freedom of Information Act 2000 (FOI), individuals can write (including by fax or email) and request access to any information public bodies hold. Under the Environmental Information Regulations 2004 (EIR), requests to public bodies for environmental information do not have to be made in writing. The CCG is subject to FOI or EIR so staff need to know how to recognise and handle such requests.

Public bodies are legally obliged to provide a response to a FOI request, including any disclosable information, within **20 working days**. All requests for information that reference FOI and EIR should be sent to the FOI administrator for logging. The FOI administrator will ensure the request is passed to the correct department and/or co-ordinate the response. If you receive a request or you are asked to respond to a request, you must deal with it in a timely manner to ensure the organisation is able to gather information and approve the request in compliance with the legal timeframe.

Information may be withheld if it falls within one of the specified exemptions in the FOI Act (known as exceptions in the Regulations). This includes information that is confidential (relating to the CCG, a partner organisation or a particular person), if it is covered by one of the data protection principles or if it would prejudice anyone's commercial interests. If the CCG withholds information, the applicant must be provided with an explanation (known as a refusal notice). That is, **ALL** applicants must receive a response regardless of whether they are provided with any information or not.

Applicants do not have to state that they are making the request under FOI or EIR so theoretically any request for information may be a request under either of these pieces of legislation. To avoid being overly bureaucratic only certain requests should be dealt with under FOI or EIR. The process for dealing with requests for information is:

- Respond to routine requests as normal in a timely manner
- FOI or EIR requests should be sent to the FOI administrator.
- A request that falls under the CCG FOI or EIR process is one which:

- ~ Specifically refers to Freedom of Information or Environmental Regulations
- ~ Requires a **Co-ordinated response**
- ~ Is **Complex** and will take a significant amount of time or effort to compile a response (this enables us to monitor the amount of time that FOI and EIR requests are taking)
- ~ Is **Contentious** (for example, the response may be about a sensitive issue in the news, you think the information may be exempt from disclosure)

- Deal with all requests for information promptly: Legislation requires that responses are sent to the applicant within 20 working days
- If you are asked to respond to a FOI or EIR request and think an exemption or exception may apply, you should contact the CCG's FOI Administrator for guidance. **All exemptions or exceptions** are applied by the Assistant Chief Officer.
- A request from an individual for information that the CCG holds about applicant which references the Freedom of Information Act (FOI) will be exempt under FOI but should be dealt with under the Data Protection Act and a response given within 40 calendar days.

Appendix 1

NHS
Rotherham
Clinical Commissioning Group

Equality Impact Assessment form 2013

Title of policy or service	Confidentiality Code of Conduct	
Name and role of officers completing the assessment	Andrew Clayton – Head of Health Informatics	
Date assessment started/completed	04.01.17	

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	In the operation of the organisation, commissioning and the delivery of effective care, the CCG obtains, holds, uses and discloses confidential information. Changes in legislation, the reconfiguration of the NHS and the diversity of service provision in the modern health care system involving close working relationships across different professional groups and health and non-health care agencies, may make it harder to understand what information it is permissible to share and in what circumstances. This code of conduct is intended to enable the CCG and its staff to work effectively in a confidential manner. It should help protect patients/service users and staff from the misuse of their information and ensure that confidential information is handled in a lawful and appropriate manner by: • Defining what is meant by "confidential information" • Informing staff of their responsibilities in relation to confidential information • Informing staff of the correct procedures for dealing with confidential information so that they do not inadvertently breach confidentiality • Providing sources of further information

2. Gathering of Information

This is the core of the analysis; what information do you have that indicates the policy or service might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			What actions do you need to take to address these issues?	What difference will this make?
	Positive Impact	**Neutral impact**	**Negative impact**		
Human rights		✓			
Age		✓			
Carers		✓			
Disability		✓			
Sex		✓			
Race		✓			
Religion or belief		✓			
Sexual orientation		✓			
Gender reassignment		✓			
Pregnancy and maternity		✓			
Marriage and civil partnership (only eliminating discrimination)		✓			
Other relevant group		✓			

Please provide details on the actions you need to take below.

3. Action plan				
Issues identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	**IG Group March 2019**		
Lead Officer	**Andrew Clayton**	**Review date:**	**March 2019**

Once complete please forward to your Equality lead Elaine Barnes via email elaine.barnes3@nhs.net