NHS
North Yorkshire
Clinical Commissioning Group

Confidentiality: Code of Conduct

November 2020

Authorship:	Senior Information Governance Officer; NECS
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	November 2020
Review Date:	November 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-109
Version Number:	1.1

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

POLICY AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Senior Information Governance Specialist	First Draft	IGSG (Nov 2020)	
0.2	Senior Information Governance Specialist	Second Draft revised for amendments from IG Steering Group		
1.0	Senior Information Governance Specialist		Approved by NHS North Yorkshire CCG Audit Committee (Nov 2020)	December 20
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

The purpose of this Code of Conduct is to lay down the key principles that staff should follow when handling personal confidential/sensitive or corporately sensitive information. All staff should to be aware of their responsibilities for safeguarding confidentiality and preserving information security and confidentiality.

2.0 Purpose

All employees working in the NHS are bound by a legal duty of confidence to protect personal and special category information they may come into contact with during the course of their work. This is not just a requirement under their contractual responsibilities but also a requirement within the common law duty of confidence, and current Data Protection Legislation and continues to exist after employment has terminated.

It is important that staff protect personal and special category, and corporately sensitive information at all times, and must therefore ensure that they are aware of and comply with all information governance policies and complete their statutory and mandatory information governance training.

3.0 Definitions / Explanation of Terms

3.1 Personal information

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

Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary. The appropriate legal basis under Article 6 of the General Data Protection Regulation must be identified and recorded in the CCG Information Asset Register to be able to legally process personal identifiable information.

3.2 Special Category Data

Special category data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

In addition to having identified a legal basis under Article 6 of the General Data Protection Regulation to legally process personal identifiable information, to legally process special category information the CCG must identify the condition under

Schedule 1 of the current Data Protection Act and the legal basis under Article 9(2) and record these on the information asset register.

4.0 Scope of the Policy

The policy applies to NHS North Yorkshire CCG and all its employees and must be followed by all those who work for the organisation, including the Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

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

5.2 SIRO

The CCG's SIRO is responsible for overseeing the implementation of appropriate processes and procedures to ensure that individuals information can be processed and held securely.

5.3 Caldicott Guardian

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

5.4 Line Manager

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

5.5 All Staff

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

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

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

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

- policy/strategy and procedure manuals;

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

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

The CCG must ensure that all contractors and supporting organisations are working to documented contracts or service level agreements that detail their responsibilities in respect of information governance and security, and confidentiality and data protection. This includes the completion of the Data Security and Protection Toolkit to a satisfactory level.

5.6 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy.

6.0 Policy Procedural Requirements

6.1 Confidentiality Principles

All staff must ensure that the following principles are adhered to:-

- Personal and special category information, and corporately confidential information must be effectively protected against improper disclosure when it is received, collected, created, stored, transmitted or disposed of.
- Access to personal confidential information or corporately confidential information must be allocated on a need-to-know basis.
- Disclosure of personal confidential information or corporately confidential information must be limited to that purpose for which the disclosure is required.
- Recipients of disclosed information must respect that it is given to them in confidence and treat it accordingly.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Where services which need to regularly or routinely share confidential information in order to provide the service must have an information sharing agreement in place, including service user information leaflets and a process to obtain consent for sharing.

Any concerns about disclosure must be discussed with either your Line Manager or the Information Governance Team.

6.2 Protecting Personal and Special Category, and Corporately Sensitive Information

The CCG is responsible for protecting all the information it holds at all times and must always be able to justify any decision to share information.

Personal confidential information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of data.

Appropriate data processing agreements need to be in place to obtain information from the relevant organisations.

Access to rooms and offices where terminals are present or personal confidential information or corporately confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of personal confidential information or corporately confidential information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular they must keep all records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing personal confidential information or corporately confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

6.3 Disclosing Personal and Special Category Information

To ensure that information is only shared with the appropriate people and in appropriate circumstances, care must be taken to check those people have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority.

- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.

Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.

If staff have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance Team.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the Information Governance team or see the Information Sharing Protocol.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail.

Transferring patient information by email to anyone outside the CCG network may only be undertaken through the NHS Mail system (i.e. from one NHSnet account to another NHSnet account or to a secure government domain e.g. gov.uk), since this ensures that mandatory government standards on encryption are met. As per the Data Protection and Confidentiality, and Email Policies.

Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

Staff should be made aware of the NHS Mail facility that allows personal confidential information to be sent securely to non- NHS Mail addresses and allows the recipient to respond in a secure manner if necessary. This should be used wherever possible when corresponding with none NHS Mail account holders where confidential information needs to be sent.

6.4 Working Away from an Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry CCG information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents, therefore appropriate measures must be taken to protect the information whilst away from organisational premises.

Taking home/ removing paper documents that contain personal confidential information or corporately confidential information from CCG premises must only be done by authorised staff and the minimum information taken. Appropriate security measures must be adopted to protect that information whilst away from organisational premises.

When working away from CCG locations staff must ensure that their working practices comply with CCG policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance.

To ensure safety of personal confidential information or corporately confidential information staff must take reasonable steps to ensure the security of that information whilst travelling and ensure that it is kept in a secure place if they take it home or to another location. Personal confidential information or corporately confidential information must be safeguarded at all times and kept in lockable locations.

Staff must minimise the amount of personal confidential information or corporately confidential information that is taken away from CCG premises.

If staff do need to carry personal confidential information or corporately confidential information they must ensure the following:

- Any personal confidential information or corporately confidential information must be carried in a suitable lockable container, etc. Prior to taking any information out, staff should consider and remember that they may be personally liable for breaches of current Data Protection Legislation and their Contract of Employment.

If staff do need to take personal confidential information or corporately confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must NOT forward any personal confidential information or corporately confidential information via email to their home e-mail account. Staff must not use or store personal confidential information or corporately confidential information on a privately owned computer or device.

6.5 Carelessness

All staff have a legal duty of confidence to keep personal confidential information or corporately confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about personal confidential information or corporately confidential information in public places or where they can be overheard.
- Leave any personal confidential information or corporately confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, and
- Leave a computer terminal logged on to a system where personal confidential information or corporately confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of personal confidential information or corporately confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed any other person. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

6.6 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the current Data Protection Legislation.

When dealing with personal confidential information or corporately confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of CCG.

If staff have concerns about this issue they should discuss it with their Line Manager or Information Governance Team.

7.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

NHS North Yorkshire CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

8.0 Consultation

This Policy has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

9.0 Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff.

10.0 Monitoring Compliance with the Document

The CCG will monitor compliance to this policy through a process of audits and the compliance safe haven checklists as required under the Data Protection and Confidentiality Policy:

11.0 Arrangements for Review

This policy will be reviewed every three years and in accordance with the following on an as and when required basis:

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

12.0 Dissemination

Staff will be made aware of the policy via the Intranet. Awareness of reviewed and amended policies will be through the CCG staff newsletter.

13.0 Associated Documentation

- Information Governance Framework and Strategy.
- Data Protection and Confidentiality Policy.
- Working From Home Guidance.
- the Department of Health Publication: Confidentiality: NHS Code of Practice November 2003;
- the Department of Health Publication Confidentiality: NHS Code of Practice – Supplementary Guidance: Public Interest Disclosures November 2010.
- HSCIC: Code of Practice on confidential information.
- HSCIC: A guide to confidentiality in health and social care.

14.0 References

This policy was developed in line with the following practices and legislation:

- Data Protection Act 2018;
- Human Rights Act 1998;
- General Data Protection Regulation 2016
- The Public Interest Disclosure Act 1998;
- Health and Social Care Act 2012 and HSC (Safety and Quality) Act 2015.
- The Computer Misuse Act 1990;
- the common law duty of confidentiality;
- National Data Guardian Standards;
- Caldicott principles;
- Information Commissioners Data Sharing Code of Practice.

15.0 Appendices

Appendix A: Confidentiality Do’s and Don’ts

16.0 Appendix A - Confidentiality Dos and Don'ts

Do's

- Do safeguard the confidentiality of all personal confidential information or corporately confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS.
- Do clear your desk at the end of each day, keeping all portable records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to personal confidential information or corporately confidential information at the end of each day, and/ or put them into a password protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for personal confidential information or corporately confidential information and ensure they have authorisation to access, and a legitimate need to know the information.
- Do share only the minimum information necessary.
- Do transfer personal confidential information or corporately confidential information securely, i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gov.uk.
- NB/ NHS.UK are not secure email addresses and should not be used for transmission of personal identifiable and confidential information.
- Do seek advice if you need to share personal confidential information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do complete statutory and mandatory training and other training as appropriate.
- Obtain and record consent for the use of data subjects personal information

Don’ts

- Don’t share passwords or smart cards, or leave them lying around for others to see or use.
- Don’t share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don’t use personal confidential or corporately confidential information unless absolutely necessary, anonymise the information where possible.
- Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.
- Don’t attempt to obtain access to personal confidential information or corporately confidential information unless you have a legitimate reason to do so.