NHS
South Warwickshire
Clinical Commissioning Group

Confidentiality Code of Conduct

VERSION CONTROL

Version:	2.0
Ratified by:	Clinical Quality and Governance
Date ratified:	28/10/2015
Name of originator/author:	Head of Patient Safety – Arden Commissioning Support Unit
Name of responsible committee:	Clinical Quality and Governance
Date last issued:	30/01/2019
Review date:	January 2022

VERSION HISTORY

Date	**Version**	**Comment / Update**
17/09/2015	1.1	Minor amendments.
03/07/2018	1.2	Amendment made by Corporate Governance Manager to update year of Data Protection Act to 2018.
24/09/2018	1.2	Amendments requested.
26/10/2018	1.3	Corrected version provided by Information Governance Officer – Arden & GEM Commissioning Support Unit. Submitted to Clinical Quality and Governance Committee.
28/11/2018	1.3	Reviewed by Clinical Quality and Governance Committee. Minor amendments requested. Recommended to Governing Body.
30/01/2019	2.0	Approved by the Governing Body.

Contents

1. Introduction

1.1. Everyone in the NHS has the responsibility to use personal information in accordance with the common law duty of confidentiality, the Data Protection Act and the Caldicott Principles. These responsibilities relate primarily to information concerning service users, but should also be applied to information concerning members of staff.

1.2. Personal data includes information about any living individual who can be identified, such as service users, health professionals, other staff, and suppliers. The information may be held in manual or electronic form, exchanged during discussions with other NHS members of staff, and seeing or overhearing confidential information about the NHS, work colleagues or individual service users.

1.3. This Code of Conduct is based on:

- Confidentiality: NHS Code of Practice (2003);
- Data Protection Act (2018);
- Freedom of Information Act (2000);
- Codes of practice issued by the Information Commissioner under section 45 and 46 of the Act;
- 'Caldicott' recommendations (1997);
- Human Rights Act (1998).

1.4. Staff are required to maintain confidentiality as outlined in various national and local documents, i.e.:

- As per individual Professional Codes of Conduct;
- Staff contracts of employment include explicit reference to these obligations and the consequences of breaches of confidentiality;
- Specific responsibilities in each person's job description;
- NHS South Warwickshire CCG's Disciplinary Policy;
- Requirements for confidentiality and security in its standing orders (and/or code of financial procedures);
- Staff handbook as part of establishing employee responsibilities;
- Use of an agency, external supplier or contractor will require them to agree (by means of a signed contract or agreement) to maintain the confidentiality and security of any personal information;
- As included in induction and other staff training materials.

2. Scope

2.1. This code applies to all CCG staff which for the purposes of this code includes but is not limited to governing body members, contractors, agency and temporary staff, student, honorary and volunteer staff.

3. Code of Conduct Principles

3.1. The CCG's Code of Conduct Principles are:

- The rights of individuals are protected and respected;
- Service users are treated with dignity and respect;
- Staff are aware that there are strict conditions under which personal data may be disclosed;
- Personal data should be kept secure and confidential at all times;
- Personal information should be anonymised wherever and whenever possible;
- Relevant precautions should be taken to maintain service user and staff confidentiality;
- If anyone is in doubt, refer to relevant policies and procedures, and if still in doubt ask your line manager;
- All staff should be aware of their responsibilities, particularly that a breach of security or infringement of confidentiality could lead to disciplinary action and even prosecution;
- Sharing of information is only carried out in line with current legislation and guidance;
- Staff will be expected to maintain confidentiality all times, including outside work locations;
- Service users and their carers are assured that their personal information and care will be kept confidential and that their privacy is respected;
- Breaches of confidentiality will be reported via the CCG incident processes;
- The seven principles of the Data Protection Act 2018 and the GDPR apply to all staff handling personal information and should be respected when handling or disclosing personal information relating to service users and members of staff. The principles are:

    1) **Accountability:** Staff take responsibility for what they do with personal data and must be able to demonstrate compliance;

    2) **Lawfulness, fairness and transparency:** Data can be processed if the data subject has **given** their consent, there is a contract, there is a legal obligation, it protects the vital interests of a person, there is a public interest, or if there is another legitimate interest;

    3) **Purpose limitation:** Data is processed for one purpose only. If data is collected for one purpose, it cannot be used for another unrelated purpose;

    4) **Data minimisation:** The data used needs to be relevant and limited to the purpose. If data is collected for HR purposes, for example, you would not ask for the employee's shoe size;

    5) **Accuracy:** Data needs to be accurate and up to date;

    6) **Storage limitation:** Data is kept for no longer than is necessary;

    7) **Integrity and confidentiality:** Protect data from unauthorised or unlawful processing and accidental loss, destruction, or damage.

- The seven Caldicott principles apply to the use of patient identifiable information. The Caldicott principles are:

    1) Justify the purpose(s) for using confidential information;

    2) Don't use personal confidential data unless it is absolutely necessary;

    3) Use the minimum necessary personal confidential data;

    4) Access to personal confidential data should be on a strict need-to-know basis;

    5) Everyone with access to personal confidential data should be aware of their responsibilities;

    6) Understand and comply with the law;

    7) Duty to Share information can be as important as the duty to protect patient confidentiality.

- In all cases, staff need to ensure that:

    - Appropriate consent will be obtained from the service user with regard to confidentiality;

    - Disclosures of personal information are made only in accordance with current policies and procedures;

    - Information must not be disclosed to the media, only specific members of the CCG have the authority to speak to the media;

    - Enquiries from relatives and friends (relating to service users and members of staff) should be handled in accordance with the wishes (consent) of the individual, taking care to identify the enquirer, and according to the CCG's Safe Haven Policy;

    - No confidential information is disclosed to their own relatives or friends.

- No information is disclosed for personal or commercial gain;

- The removal of personal details alone may be insufficient to protect a service user's identity – if in doubt seek the advice of your line manager or the CSU IG Consultant;

- They remain vigilant to the possibility of people seeking information by deception - take particular care when dealing with telephone requests for personal information relating to both service users and staff;

- They comply with policies and procedures for transmitting patient- identifiable information by any means, ensuring that the risks of information going astray or being seen by someone else are kept to a minimum, e.g. ensure 'Safe Haven' procedures are adhered to;

- They use email in accordance with the CCG policy and procedures;

- The Data Protection Act (2018) and Human Rights Act (1998) are respected, in particular the right to respect for private and family life.

3.2. For further information, staff should contact one of the following:

- The CCG's Corporate Governance Manager;
- The CSU's IG Consultant;
- The CCG's Caldicott Guardian;
- The CCG's Data Protection Officer (DPO).

4. Roles and Responsibilities

4.1. The CCG's Accountable Officer has the ultimate responsibility for compliance with the data protection legislation regarding the confidentiality of personal data.

4.2. The Caldicott Guardian is the senior staff member appointed to protect patient information and advise on options for lawful and ethical processing of information. They act as the Acting as the 'conscience' of an organisation.

4.3. The Senior Information Risk Officer (SIRO) is responsible for ensuring information risk is managed.

4.4. The Corporate Governance Manager supports the Caldicott Guardian and SIRO to ensure the confidentiality work programme is implemented and provides regular reports to senior management. They ensure the CCG adheres to the data protection legislation, maintaining notification, developing policies and guidance for staff and providing advice to staff.

4.5. The Data Protection Officer (DPO) is a natural, identifiable person responsible for informing and advising the organisation and its employees of their obligations pursuant to the GDPR and national data protection legislation, and monitoring compliance, reporting to the highest management level of the organisation – i.e. board level. It is a primary contact for data subjects and the Information Commissioner's Office (ICO). CCG staff consult the DPO when, for example, conducting a Data Protection Impact Assessment (DPIA) and when serious personal data breaches need to be reported to the ICO.

4.6. The CSU's Information Governance team provides advice and guidance in respect of Confidentiality.

4.7. Every staff member is responsible for processing personal data, special category data and corporate data in a confidential manner, for reporting all breaches of confidentiality – both near misses and incidents.

5. Equality & Diversity Impact Assessment

5.1. In reviewing this Code, the CCG considered, as a minimum, the following questions:

- Are the aims of this Code clear?
- Are responsibilities clearly identified?
- Has the Code been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?

- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so, is this planned?

5.2. Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy, race, religion or belief, sex, sexual orientation. No adverse impacts have been identified.

6. Monitoring Compliance and Effectiveness of the Code

6.1. The Clinical Quality and Governance Committee will be informed of any identified breaches of the Code.

6.2. This Code will be reviewed every three years by the Clinical Quality and Governance Committee.

7. References and Further Reading

7.1. This Code should be read in conjunction with the following:

- Records Management Policy;
- Records Management Strategy;
- Freedom of Information Policy and Procedures;
- Information Security Policy;
- Email Usage Policy;
- Internet Usage Policy;
- Remote Working Policy
- Safe Haven Policy and Procedure;
- Coventry and Warwickshire-Wide Sharing of Information Protocols;
- Confidentiality and Data Protection Policy;
- Disciplinary Policy;
- Complaints Management ProcedurePolicy;
- Whistleblowing Policy;
- Grievance Policy.

End of Document