IG06 – Code of Confidentiality

Corby and Nene Clinical Commissioning Groups

Version 5

Document revision history

Date	Version	Revision	Comment	Author/Editor
08/05/2018	4.1	Review	GDPR update	Senior Internal and Assurance IG Manager
17/05/2018	4.1a	Prior to CCG review and adoption	Edited for use by Nene CCG To replace IG16v4.0 Need to check CCG email address (section 6), CCG job descriptions (section 12)	John Geaney, IG Compliance Manager
18/05/2018	4.1b	CCG Review	Edited to cover both Nene and Corby CCGs and minor revisions	Information Manager

Document approval

Date	Version	Revision	Role of approver	Approver
July 2018	5.0	Final		Corby and Nene Audit and Risk Committees

Contents

1.0 Introduction

This code of conduct has been produced to ensure that all Corby and Nene CCG staff members are aware of their legal duty to maintain confidentiality and the processes in place to protect personal and sensitive corporate information. It also provides guidance on the processes to be followed when information is legally disclosed.

Everyone working for the CCGs is under a legal and contractual duty to protect the confidentiality of personal information. This duty also extends to commercially sensitive corporate information where the legitimate business interests or operations of Corby and Nene CCG could be damaged or hindered by unauthorised disclosure. Members of the public (including staff) who believe their privacy has been breached may make a complaint to the CCG and could take legal action against the organization(s) and/or individuals responsible for the breach.

This code of conduct is supplementary to the National Confidentiality: NHS Code of Practice – Department of Health

2.0 Scope

The code is concerned with protecting personal information about service users and employees and also commercially sensitive corporate information about legitimate business processes; its content applies equally to personal information about members of staff.

Personal information is data in any form from which a living individual could be identified: paper, electronic, voice recording, oral (conversations held in open areas). It includes pictures of individuals, their name, age, address, and personal circumstances, as well as sensitive personal information such as race, health, sexuality, etc. The Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation, only covers the personal information of living individuals, this code also applies to information about deceased service users.

Anonymised data, which does not consist of personal information, is still owed a duty of confidence (in accordance to NHS Digital's Guide to Confidentiality) and therefore staff should still ensure that the necessary controls are in place prior to sending anonymised data to a third party or outside of the organisation. Although there is no personal identifiable information available within the dataset, the dataset itself may contain items which may identify an individual if reviewed and compared with other data. Please contact the Information Governance Team for assessment and guidance.

Staff must comply with the requirements of all health and social care legislation that relates to the delivery of services; in particular, the Health and Social Care Act 2012 and Care Act 2014, both Acts specifically define the limits on personal information available to specific types of Healthcare Providers, Commissioners and their supporting organisations – such as Corby CCG and Nene CCG.

Commercially sensitive corporate information includes – but is not limited to – business strategies and plans (both final and draft), operational budgets, quotes, tenders, contracts, legal advice and investigations. All of which would not normally be considered for general release or publication under the Freedom of Information Act (2000) unless there was an overriding public interest exemption.

The code applies to all staff, including permanent, temporary, student, volunteers and locum members of staff. It continues to apply even when they are no longer working for the CCG, no matter how much time has elapsed.

3.0 Definitions

- **Controller** (DPA Part 3, Ch. 1, s.32): controller means a competent authority who (either alone or jointly with another competent authority) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed.

- **Processor** (DPA Part 3, Ch. 1, s.32): processor means any organisation (other than an employee of the controller) that processes personal data on behalf of the controller.

More detail on these definitions and the legal justification for processing is noted in section 13, below.

The CCGs are processors for any personal or sensitive information held on behalf of its customers; for example:

- CCG electronic files relating to their employees or patients
- Data from NHS Digital relating to patients, or pseudonymised data with a weak identifier (e.g. NHS number)
- Hospital/Mental Health Trust files relating to their employees or patients.

4.0 Professional obligations

A duty of confidentiality is a legal obligation for registered health professionals; it arises out of the common law duty of confidentiality and forms part of employment contracts. Breaches of confidentiality and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal prosecution[1].

Make sure you do not[2]:

- put personal information at risk of unauthorised access
- knowingly misuse any personal information or allow others to do so
- access records or information that you have no legitimate reason to look at; this includes records and information about yourself, your family, friends, neighbours and acquaintances.

5.0 Corporate information

Make sure you comply with the following staff guidelines made available on the intranet which set out practical things you should do to protect personal and commercially sensitive corporate information:

- good record keeping (*see* information management protocol and document procedures)
- appropriate use of computer systems (*see* access control procedures)
- secure use of personal information (see ICT Acceptable Use Policy)
- reporting information incidents (*see* incident management procedure)
- using mobile computing devices securely (see ICT Acceptable Use Policy).

6.0 Processes for disclosure

Under normal circumstances, CCG staff must not release personal or commercially sensitive corporate information: requests for personal information should be directed to the relevant customer as the controller; requests for corporate information should be directed to appropriately authorised Corby CCG and Nene CCG managers.

A series of posters and leaflets detailing disclosure processes will be issued to staff as part of information governance awareness raising and training programmes. These will tell staff why, how, and for what purpose personal and corporate commercially sensitive information is collected, recorded and used by the CCGs.

[1] Data Protection Act 2018, including the General Data Protection Regulation (EU) 2016/6 and Common Law Duty of Confidentiality

[2] Confidentiality: NHS Code of Practice – Department of Health

You must ensure you are familiar with this material and ask for advice from the Information Governance Team if you are unable to answer any questions.

If you are authorised to disclose personal or corporate commercially sensitive information, you must ensure you do so in accordance with the information handling procedures. These require you to:

- share only with those with a legitimate right to see/hear the information
- transfer in accordance with the organisation's secure transfer methods
- disclose the minimum necessary to meet the scope of the request.

If you are authorised to disclose information that can identify an individual patient for non-healthcare purposes (e.g. research, financial payment/audit), you must do so only if one of the following applies:

- you have the patient's explicit consent
- the consent is written – to ensure there is no later dispute about whether consent was given
- the disclosure was required by a court order.

Under the common law duty of confidentiality, identifiable personal information may be disclosed without consent in certain circumstances. These are:

- where there is a legal justification for doing so, e.g. to comply with a statute, such as reporting knife crimes
- where there is a public interest justification: e.g. where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the patient concerned and the broader public interest in the provision of confidential service.

You must refer all requests for disclosure of personal information without the consent of the service user, including requests from the police or a court, to the CCG Information Governance Team:
nccg.informationgovernance@nhs.net

7.0 Training

All staff will be made aware of their responsibilities for information security through generic and specific training programmes and guidance. Training requirements will be publicised via the communications department.

The ICT Security Manager is responsible for ensuring ICT security awareness and training for all staff.

8.0 Monitoring and compliance

This policy and the associated controls will be monitored through the risk management system for the CCGs. The risk register will be reviewed frequently and, also, in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a priority for the information governance work plan; wider assurance and control are a key component of this.

Information risk owners, assisted by information risk administrators, will be required to routinely review the risks and information flows associated with the information assets utilised to fulfil the business functions and activities within their remit.

Further monitoring will be undertaken through the change control process.

Table 1: Control Audit and Monitoring Table

What we must monitor	• The management of information risks (Information Risk Management) • Compliance with the law • Compliance with the Data Security and Protection (DSP) Toolkit • Incidents related to the breach of this code of conduct
Monitoring method	• Information risks will be monitored through the risk management system. • Compliance with law will be monitored through audit, work directed by the DSP Toolkit and as directed by the CCG Group and Information Governance Working Group • In addition, the DSP Toolkit will be audited by the organisation's internal audit function before the annual submission. • Incident reporting and management requirements
Responsibility for monitoring	• Information Governance Team • Incident reports will be produced by the nominated investigation officer
Oversight of monitoring reports	• Information Governance Working Group • Senior Information Risk Owner • Caldicott Guardian • Highlight report for escalation to the Performance and Delivery CCG Group, where required
Frequency of review	• Monthly updates will be provided to the CCG Group, IG Working Group, the SIRO and the CG • The internal audit report on DSP Toolkit performance will be provided to the CCG Group. • Incident Reports will be reviewed on a monthly/quarterly/annual basis and as directed according to the seriousness of the incident

Non-compliance

Disciplinary action may be taken in response to any failure to comply with the standards and appropriate governance of information, supporting protocols and procedures as detailed in this policy. All staff are reminded that this policy covers several aspects of legal compliance that they are responsible for as individuals. Failure to maintain these standards can result in criminal proceedings against the individual. These include, but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958
- Health and Social Care Act 2012
- Care Act 2014
- Confidentiality: NHS Code of Practice – Department of Health

9.0 Review

A review of this code of confidentiality will take place every three years or earlier, until rescinded or superseded due to legal or national policy changes.

Those referring to this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available in the policy register for the organisation. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

10.0 Implementation and dissemination

The confidentiality code of conduct will be shared with all staff through the all-staff email, updated on the intranet where this is available, included in staff briefings and placed in the policy register. A team and management briefing will support this dissemination.

In addition to the monitoring detailed above, awareness of the code will be checked through a staff survey and spot checks on at least an annual basis.

11.0 Acknowledgement

By signing below, I acknowledge that I have read and understand the CCG's Confidentiality Code of Conduct.

Name:	
Signature:	
Date:	

12.0 Equality Impact Assessment

The CCG aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It considers current UK legislative requirements, including the Equality Act 2010 and the human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identify, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the CCG must have due regard to the Public-Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

The purpose of this assessment is to assess the likely (or actual) effects of this policy on people in respect of disability, gender, including gender identity, racial equality and wider equality areas including looking for opportunities to promote equality, as well as negative or adverse impacts that can be removed or mitigated.

A full impact assessment will normally be required if you have answered YES to one or more of questions 1, 2 and 3 below.

1	Does the policy meet any of the following duties/needs:	
	• Eliminate unlawful discrimination, harassment and victimisation.	**No**
	• Advance equality of opportunity between people who share a protected characteristic and those who do not.	**No**
	• Foster good relations between people who share a protected characteristic and those who do not.	**No**
2	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any group/s*?	**No**
3	Is there any evidence or other reason to believe that different groups* have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?	**No**
4	Has prior consultation taken place with organisations or groups* which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?	**No**

* Race/ ethnicity, gender (including gender reassignment) age, religion or belief, disability, sexual orientation, marriage or civil partnership, pregnancy and maternity. This will include groups such as refugees and asylum seekers, new migrants, Gypsy and Traveller communities; and people with long term conditions, hearing or visual impairment

13.0 The conditions (the legal basis) for processing Personal Data under the Data Protection Legislation

The conditions for processing Personal Data and Sensitive Personal Data the Data Protection Legislation, Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation.

Definition of Personal Data and Sensitive Personal Data
Data:

- The Data Protection Act defines data as:
  - Information which is being processed automatically in response to instruction
  - Information recorded as part of a highly structured filing system (e.g. an individual with limited knowledge of the filing structure could logically retrieve relevant information)
  - Recorded information held by a public authority
  - Information that forms part of an accessible record (health, educational, public record)

Personal Data:

- Personal data means data which relates to a living person who can be identified from that set of data or who could be identified if that data was combined with other information either available or likely to become available.
- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Sensitive Personal Data
The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Special Categories of personal data includes Information relating to the data subjects’:

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- trade union membership,
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act (DPA) outlines 6 principles for handling Personal Confidential Data (PCD), with 2 additional safeguards:

1. Data must be processed fairly and lawfully
2. Data must be obtained and processed only for one or more specified and lawful purposes
3. Date must be adequate, relevant and not excessive in relation to the purpose
4. Data must be accurate and kept up to date
5. Data must not be kept for longer than is necessary
6. Appropriate technical and organisational security measures for the data must be in place

Safeguards:

1. Data must be processed in accordance with the rights of data subjects
2. Sensitive Data must only be processed with legal compliance to the Act, referenced to a current policy. e.g. Can only be processed in a country or territory outside the United Kingdom unless adequate levels of protection are in place, within statutory functions.