South East London CCG
Confidentiality Policy

Document revision history

Date	Version	Revision	Comment	Author/Editor
14/01/2020	V0.1	Reviewed and tailored for SEL CCG	Draft	IG Compliance Manager
20/01/2020	V0.2	Bexley CCG	Draft	IG Support Officer
06/02/2020	V0.3	Additional amends	Draft	IG Support Officer/IG Compliance Manager
11/02/2020	V0.4	Final amends and formatting	Draft	IG Compliance Manager
26/02/2020	V1.0	Document finalised	Final	IG Compliance Manager

Document approval

Date	Version	Revision	Role of approver	Approver
26/02/2020	V1.0	Document finalised	IGSG	IGSG

Contents

1.0 Introduction

1.1 The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within NHS South East London Clinical Commissioning Group (hereafter referred to as 'the CCG') and have access to personal data or confidential information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security.

1.2 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 2018. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

1.3 It is important that the CCG protects and safeguards personal data and confidential business information that it gathers, creates, processes and discloses, in order to comply with the law, relevant NHS mandatory requirements, with the aim to ensure individual's rights to privacy are respected.

1.4 This policy sets out the requirements placed on all staff when processing and sharing information within the NHS and between NHS and non-NHS organisations.

1.5 Personal data is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, which must not be stored on removable media unless it is encrypted as per current NHS encryption guidance or a business case has been approved by the Information Governance Team.

1.6 Personal data may include special categories of personal data or criminal convictions and offences data. Special categories of personal data are considered to be more sensitive and therefore must only be processed in limited circumstances. It can take many forms, including individuals' health and mental health, sex life/sexual orientation, ethnic origin, political options, religious beliefs, genetic and biometric information.

1.7 Confidential information encompasses the above and within the NHS, it can include information that is private and not public knowledge, or information that an individual or an organisation would not expect to be shared. This includes CCG confidential business information.

1.8 Information can relate to individuals (including staff and temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, mobile devices, digital cameras or even heard or recorded verbally.

1.9 For the purpose of this policy, the above categories of information are defined as personal data and confidential information.

1.10 This policy is supported by further information in the appendices and other NHS South East London CCG information governance policies and guidance.

2.0 Scope

2.1 This policy applies to all CCG staff and agents acting on behalf of the organisation.

3.0 Roles and responsibilities

3.1 Confidentiality and data protection is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003 and data protection legislation. There are confidentiality and data protection clauses in all staff contracts, and all staff are obliged to participate

in induction, training and awareness-raising sessions carried out to inform and update staff on confidentiality and data protection responsibilities.

3.2 Designated roles and responsibilities are outlined within the CCG's Information Governance Framework.

3.3 Any breach of confidentiality or data protection, inappropriate use of individuals'/staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported in line with the Information Security Policy.

4.0 Key principles

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

- Personal data and confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to personal data or confidential information must be on a need-to-know basis.
- Disclosure of personal data or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either your line manager or the Information Governance Team.
- Understand what constitutes a data breach or near miss and ensure the appropriate action is taken to report the breach and escalate any issues.

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

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

5.0 Disclosing personal/confidential information

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

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

5.3 Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Office's Anonymisation Code of Practice.
- When the information is required by law or under a court order. In this situation staff, must discuss with their line manager or Information Governance staff before disclosing, who will inform 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. Referred to as approval under s251 of the NHS Act 2006.

- 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 or Information Governance staff before disclosing, who will inform and obtain the 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 or Information Governance Team before disclosing, who will inform and obtain approval from the Caldicott Guardian.

5.4 If staff have any concerns about disclosing information, they must discuss this with their line manager or the Information Governance Team.

5.5 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/information 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.

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

5.7 Transferring patient information by email to anyone outside the CCG network may only be undertaken by using encryption as per the current NHS encryption guidance or through an exchange within the list of NHS Digital approved mail systems (i.e. from a CCG email account to another NHS.net account or to a secure government domain e.g. gsi.gov.uk), since this ensures that mandatory government standards on encryption are met. 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 personal data or confidential information.

6.0 Security measures and access controls

6.1 The CCG will have appropriate security measures in place to guard against:

- Unauthorised access to, alteration, disclosure and destruction of data; and
- Accidental loss or destruction.

6.2 The CCG will ensure through its documented policies and procedures that only authorised individuals can gain access to its systems and records.

6.3 All equipment, records and storage media will be protected from inappropriate and unauthorised access by physical and electronic security measures. The sharing, copying, archiving or destruction of any data, electronic, paper or other media will be treated with the same level of security.

6.4 Access to rooms and offices where terminals are present or personal data or 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 data by unauthorised parties.

6.5 Further information regarding the CCG's security measures will be detailed in the Information Security Policy and the ICT security policies held by the CCG's ICT providers.

7.0 Working away from the office environment

7.1 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 the CCG's information with them, which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

7.2 Taking home/removing paper documents that contain personal data or confidential information from CCG premises is discouraged.

7.3 To ensure safety of confidential information, staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

7.4 When working away from CCG locations, staff must ensure that their working practice complies with organisational policies and procedures. Any electronic removable media must be encrypted as per the current NHS encryption guidance.

7.5 Staff must minimise the amount of personal data that is taken away from CCG premises.

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

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of CCG buildings; and
- Confidential information is kept out of sight whilst being transported.

7.7 If staff do need to take personal data or confidential information home, they have a 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.

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

7.9 Further information is available in the Mobile devices and remote working policy.

8.0 Carelessness

8.1 All staff have a legal duty of confidence to keep personal data or confidential information private and not to divulge information accidentally.

8.2 Staff may be held personally liable for a breach of confidence and must not:

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

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

8.4 Passwords must be kept secure and must not be disclosed to unauthorised persons. 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. If you allow another person to use your password to access the network, this constitutes gross misconduct which may result in your dismissal.

9.0 Abuse of privilege

9.1 It is strictly forbidden for employees to knowingly browse, search for or look at any personal data 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 Data Protection Act.

9.2 When dealing with personal data or 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 the CCG.

9.3 If staff have concerns about this issue, they should discuss it with their line manager or Information Governance Team.

10.0 Confidentiality audits

10.1 Good practice requires that all organisations that handle personal data or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the Information Governance Team through a programme of audits.

10.2 Staff must be made aware that the CCG will complete security audits and spot checks of its systems and activities to prevent any unauthorised access of misuse of personal data or confidential information. Any misconduct can lead to disciplinary action being taken.

11.0 Distribution and implementation

11.1 This document will be made available to all staff via the CCG intranet site.

11.2 A global notice will be sent to all staff notifying them of the release of this document.

12.0 Monitoring

12.1 Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Team, together with independent reviews by both internal and external audit on a periodic basis.

12.2 The Information Governance Team is responsible for the monitoring, revision and updating of this document on a three yearly basis or sooner if the need arises.

Appendix A: Confidentiality Dos and Don'ts

Do

- Do safeguard the confidentiality of all personal data or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of the CCG.
- Do clear your desk at the end of each day, keeping all portable records containing personal data or 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 data or business confidential information, 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 data or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer personal data or confidential information securely when necessary i.e. use a CCG email account to send confidential information to an nhs.net email account, a secure government domain e.g. gsi.gov.uk, or to an NHS Digital approved email domain.
- Do seek advice if you need to share personal data without the consent of the identifiable person's consent and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness-raising sessions on confidentiality issues.
- Do put confidential documents in the designated confidential waste bins or shred the documentation using the facilities provided.

Don't

- Don't share passwords or leave them lying around for others to see.
- 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 data 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 leave unwanted printouts containing personal data or confidential information unattended.

Appendix B: Summary of Legal and NHS Mandated Frameworks

NHS South East London Clinical Commissioning Group is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the organisation, who may be held personally accountable for any breaches of information security for which they may be held responsible.

Legislation and guidance

The Data Protection Act 2018 regulates the use of "personal data" and sets out six principles to ensure that personal data is:

1. Processed lawfully, fairly and transparently;
2. Processed for specific, explicit and legitimate purposes;
3. Adequate, relevant and not excessive;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary; and
6. Processed in a secure manner.

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information;
- Don't use patient identifiable information unless it is absolutely necessary;
- Use the minimum necessary patient-identifiable information;
- Access to patient-identifiable information should be on a strict need to know basis;
- Everyone should be aware of their responsibilities;
- Understand and comply with the law; and
- The duty to share information can be as important as the duty to protect patient confidentiality.

Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

The NHS Confidentiality Code of Practice (2003) outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information;
- Inform patients of how their information is used;

- Allow patients to decide whether their information can be shared; and
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality means that information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers.

The NHS Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

> *Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:*
>
> - *You ask us to do so;*
> - *We ask and you give us specific permission;*
> - *We have to do this by law;*
> - *We have special permission for health or research purposes; or*
> - *We have special permission because the public good is thought to be of greater importance than your confidentiality; and*
> - *If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.*
>
> *Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.*

The Access to Health Records Act 1990 provides certain individuals with a right of access to the health records of a deceased individual. These individuals are defined under Section 3(1)(f) of that Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.

Appendix C: Definitions

Personal data is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive/confidential personal information as defined by the Data Protection Act 2018 refers to personal information about:

- Race or ethnic origin;
- Political opinions;
- Religious or similar beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for purpose of uniquely identifying a living person;
- Physical or mental health or condition; or
- Sexual life/orientation.

Non-personal data can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.