Confidentiality Policy

Version 0.4

Document revision history

Date	Version	Revision	Comment	Author/Editor
03/10/2018	V0.1	Draft GDPR compliant document created	DRAFT	Head of Information Governance
14/11/2018	V0.2	Revisions	Draft	IGSG Meeting/Merton CCG
07.12.2018	V 0.3	Revision	Draft	IGSG Meeting/Merton CCG

Document approval

Date	Version	Revision	Role of approver	Approver
31.12.18	V.04	Final	Information Governance Steering Group Meeting	Caldicott Guardian /Senior Information Risk Owner Merton & Wandsworth CCG

Contents

CONTENTS 3

1. INTRODUCTION 4

2. SCOPE 5

4. KEY PRINCIPLES 5

5. DISCLOSING PERSONAL/CONFIDENTIAL INFORMATION 6

6. WORKING AWAY FROM THE OFFICE ENVIRONMENT 8

7. CARELESSNESS 9

8. ABUSE OF PRIVILEGE 9

9. BREACHES 10

10. CONFIDENTIALITY AUDITS 10

11. DISTRIBUTION AND IMPLEMENTATION 10

12. MONITORING 10

13. EQUALITY IMPACT ASSESSMENT 11

APPENDIX A: CONFIDENTIALITY DOS AND DON'TS 12

APPENDIX B: SUMMARY OF LEGAL AND NHS MANDATED FRAMEWORKS 13

APPENDIX C: DEFINITIONS 16

1. Introduction

1.1 The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all staff who work within the CCGs and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. This document is also part of a suite of Policies listed in the Information Governance Framework Policy of Merton and Wandsworth CCG.

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 1998. 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 CCGs protects and safeguards person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

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

1.5 Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and 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 Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes the CCGs confidential business information.

1.7 Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

1.8 A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

1.9 The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

1.10 How to report a breach of this policy and what should be reported can be found in Appendix C.

1.11 Definitions of confidential information can be found in Appendix D.

2. Scope

This policy applies to all CCGs staff and agents acting on behalf of the CCGs. This includes Contractors, temporary staff, secondees and all permanent employees. (For more information please review the Information Governance Framework Policy)

3. Roles and Responsibilities

3.1 Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

3.2 Specific roles and responsibilities are outlined within the Information Governance Framework Policy.

4. Key Principles

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

- Person identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable 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.

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

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

4.4 Access to rooms and offices where terminals are present or person identifiable 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 person-identifiable information by unauthorised parties.

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

4.6 Unwanted printouts containing person-identifiable or 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.

4.7 The 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.

5. 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 to ensure only the minimal amount necessary is disclosed.

5.3 Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Officer 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 staff before disclosing, who will inform and obtain approval of 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 staff.

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, faxes and surface mail.

5.7 Transferring patient information by email to anyone outside the CGGs network may only be undertaken by using encryption as per the current NHS Encryption Guidance or through an exchange within the NHS Mail system (i.e. from one NHS.net 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 person-identifiable or confidential information.

6. Working Away from the Office Environment

6.1 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 CCGs information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

6.2 Taking home/ removing paper documents that contain person-identifiable or confidential information from CCG premises is discouraged.

6.3 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.

6.4 When working away from CCGs locations staff must ensure that their working practice complies with the CCG's policies and procedures. Any electronic removable media must be encrypted as per the current NHS Encryption Guidance.

6.5 Staff must minimise the amount of person-identifiable information that is taken away from CCG premises.

6.6 If staff do need to carry person-identifiable 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 CCGs buildings.
- Confidential information is kept out of sight whilst being transported.

6.7 If staff do need to take person-identifiable or 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.

6.8 Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately owned computer or device. Staff may be held liable for breaches of confidentiality which will be subject to the CCG's disciplinary procedure.

7. Carelessness

7.1 All staff have a legal duty of confidence to keep person-identifiable or 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 person identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, by an unauthorised individual.

7.2 Steps must be taken by the employee and employer to ensure physical safety and security of person identifiable or business confidential information held in paper format and on computers.

7.3 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 a member of staff allows another person to use their own password to access the network, this constitutes a disciplinary offence. This is gross misconduct which may result in summary dismissal.

8. Abuse of Privilege

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

8.2 When dealing with person-identifiable 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.

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

9. Breaches

9.1 Any breach of confidentiality, inappropriate use of health, 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.

9.2 Under Article 33 of the General Data Protection Regulations (2018) personal breach notifications must be reported to the Information Commissioners Office (ICO) within 72 hours where there may be a risk to data subjects. Any data breach must be reported to the CCG's Data Protection Officer and the SIRO immediately on identification or knowledge of a possible breach of confidentiality.

10. Confidentiality Audits

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems. Procedures to evaluate the effectiveness of controls within these systems should be regularly scheduled. This function will be co-ordinated by the Information Governance team through a programme of audits.

11. Distribution and Implementation

11.1 This document will be made available to all Staff via the CCGs intranet site.

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

11.3 A link to this document will be provided on Workforce and in every employee's Company handbook or contract on confirmation of employment with the CCGs whether on a permanent, temporary or contract basis.

12. 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 3 yearly basis or sooner if the need arises.

13. Equality Impact Assessment

This document forms part of Merton/Wandsworth CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to all protective characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity,) and in addition to offending background, trade union membership or political affiliation .This is to promote positive practice and value the diversity of all individuals and communities.

Appendix A: Confidentiality Dos and Don'ts

Dos

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of the CCGs.

- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable 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 person-identifiable 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 person-identifiable or confidential information and ensure they have a need to know.

- Do share only the minimum information necessary.

- Do transfer person-identifiable or confidential information securely when necessary 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. gsi.gov.uk.

- Do seek advice if you need to share patient/person-identifiable 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 participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- 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 person-identifiable 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.

Appendix B: Summary of Legal and NHS Mandated Frameworks

The CCGs are 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 CCGs, who may be held personally accountable for any breaches of information security for which they may be held responsible.

Legislation and guidance

Data Protection Act 2018 regulates the use of "personal data" and sets out six principles which have the following requirements:-

1. Processing must have a lawful basis and be fair;

2. Processing must be specific , explicit and legitimate;
3. Personal data be adequate, relevant and not excessive;
4. Personal data be accurate and kept up to date;
5. Personal data be kept for no longer than is necessary;
6. Personal data must be processed in a secure manner.

In addition to these principles there is a requirement that the CCG's as Data Processors and Controllers are accountable, responsible for and must be able to demonstrate compliance with these principles.

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.
- 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.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

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

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

The 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.

Appendix C: Definitions

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 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
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission 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

Non-person-identifiable information 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.