Tower Hamlets GP Care Group (THGPCG) CIC Policy CONFIDENTIALITY CODE OF PRACTICE	
Category	Information Governance
Policy drafted by	Phalguni Trivedi
Policy Approved by Operational Lead and date	
Policy approved by Board Lead and date	Dr Joe Hall, Dr S Shan, Lisa Henschen and Ayesha Lulat Governance Lead
Date for review	01/08/2015

Introduction

This policy sets out the required standards for all GP Care Group staff members in order to ensure and maintain the confidentiality of patient information.

The purpose of this document is to provide staff with a clear code of conduct for confidentiality. It is the responsibility of all staff to adhere to this code of conduct. All staff are bound by a legal duty of confidentiality. This means they are obliged to keep strictly confidential any person identifiable information (patient and / or staff), commercially sensitive or business in confidence details they become party to.

The principle behind this code of conduct is that no member of staff shall breach their legal duty of confidentiality, allow others to do so, or attempt to defeat any of the GP Care Group security systems or controls in order to do so. This code of conduct forms part of the Information Governance framework and is based on the Caldicott principles

Applicability

This policy applies to:

All staff i.e. GP Care Group staff, agency staff, directors and any other persons working for GP care Group, such as persons engaged on GP Care group business or persons using GP care group equipment and/ or networks.

This is not an exhaustive list as the policy applies to anyone that has dealings with the GP Care Group.

1. **PROTECT PATIENT INFORMATION**

1.1. Patients' health information must be protected through a number of measures:

- Ensure all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality
- Record patient information accurately and consistently
- Keep patient information confidential
- Keep patient information physically secure
- Disclose and use information with appropriate care
- Ensure that disclosure of information passed outside the GP Care Group is in accordance with the Caldicott Principles and the Data Protection Act 1998.

1.2 Patient identifiable Information - Key identifiable information includes:

- Patient's name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients;
- NHS number and local patient identifiable codes; and
- Anything else that may be used to identify a patient directly or indirectly.

2. **INFORM PATIENTS EFFECTIVELY**

The GP Care Group must actively inform patients of the intended use of their information, give them the choice to give or withhold their consent and protect their identifiable information from unwarranted disclosure.

2.1 Staff should consider situations in which patients would be surprised to learn that their information was being used in a particular way – if so, they are not being effectively informed.

2.2 Whenever possible all staff must make clear to patients how their information is used or shared to provide the best possible care. Comments like the following might be appropriate:

- Make it clear to patients how their information is recorded in their health records and on the computer system(s)
- Be open and honest with the patient on what information is recorded in their health records
- Whenever possible all staff must make it clear to patients how their information is used or shared to provide the best possible care, this may require no more than a comment such as: When writing a referral letter explain to the patient - 'I am going to refer your details to physiotherapy who will contact you to arrange a course of therapy'
- When entering information into an electronic record explain to the patient what you are entering and who will be able to view this information.
- Inform patients that they have the right to know, and possibly object to how their information may be disclosed/shared

- Ensure that patients have no concerns or queries about how their information is disclosed and used
- Answer any queries, or direct a patient to others who can answer their questions, about how their information is used
- Respect the rights of patients and facilitate them in exercising their rights to have access to their health records, where applicable.

3. PATIENT CONSENT TO DISCLOSURE

3.1 Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. Staff must:

- Seek the patient's consent prior to using their information in ways that do not directly contribute, or support the delivery of their care
- Respect a patient's decisions to restrict the disclosure or use of their information, expect where exceptional circumstances apply
- Communicate effectively with patients to ensure they understand the implications if they choose to agree or restrict the disclosure of their information.

3.2 All staff should be aware that patients have the right to object to the use and disclosure of confidential information that identifies them. Staff must therefore be provided with training on how to seek and record consent from patients on the use of their medical records.

3.3 If they are unable to answer the questions or concerns, staff should be able to direct the questions or concerns to their line manager or another member of staff who can provide the answer. If the line manager or other team member is unable to answer the questions or concerns, advice and guidance can be sought from the Caldicott Guardian or other appropriate member of the IG Committee.

4. IMPROVING CONFIDENTIALITY

4.1 Staff must:

- Be aware of the issues surrounding confidentiality, and seek training and support when uncertain on how to deal with these issues
- Report all possible or risk of breaches of confidentiality
- Ensure that they apply the Caldicott principles every time they are sharing information.

4.2 The confidentiality model outlines the requirements that must be met in order to provide patients with a confidential service. Staff must inform patients of the intended use of their information, give them the choice to give or withhold their consent, as well as protecting their identifiable information from

unwarranted disclosures. These processes are inter-linked and should be on going to aid the improvement of a confidential service.

The four main requirements are:

- PROTECT – look after the person identifiable information
- INFORM – ensure that patients are aware of how their information is used
- PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways
- IMPROVE – always look for better ways to protect, inform and provide choice

5. EXCEPTIONAL CIRCUMSTANCES

5.1 Exceptional Circumstances where disclosure may be permitted are detailed in professional bodies' guidance. Information can be disclosed without patient consent:

- o where there is a risk of death or serious harm to others e.g. a patient who drives contrary to medical advice
- o where there is a statutory duty e.g. in the case of a patient with a notifiable disease, Reporting of Injuries Diseases and Dangerous Occurrences Regulations (RIDDOR)
- o when required to do so by a court order

5.2 Where a patient is a victim of neglect, physical or sexual abuse reference should be made to the identification of inadequate care and protection of 'adults at risk' from abuse safeguarding adults)Adults Policy, which covers the difficult issue of consent in these circumstances.

5.3 When information is disclosed without a patient's consent, this must be recorded in the patient's health record and the member of staff must be prepared to justify their decision for disclosing patient information without consent.

Children and young people

5.4 Children under the age of 16 who are competent to make decisions about their own treatment without parental involvement are also competent to make decisions about the use and disclosure of information they have provided in confidence

5.5 A clinician who discloses information in these circumstances must be prepared to justify his or her reasons for doing so. The child should be told that information will be disclosed and the reasons for it. The amount of information disclosed should be the minimum necessary to enable an appropriate inquiry to be carried out. Reference should also be made to the GP Care Group Child Protection Policy.

5.6 Where a child is not able to fully understand the nature and purpose for disclosing information, a person with parental responsibility should be approached to obtain consent. However, it is considered good practice to obtain the child's

views on the disclosure of their information.

5.7 Where there are reasonable grounds for believing that a child is at risk of or has suffered significant harm e.g. as a result of physical or sexual abuse, the healthcare professional should disclose information to the appropriate authorities. He or she should attempt to obtain consent for this unless to do so would place the child at risk of serious harm. Where information is disclosed, the healthcare professional must be able to demonstrate the information disclosure had been carefully considered and was in the best interests of the child. The child and family should be informed of the disclosure unless to do so would place the child at risk of serious harm

Complaints

5.8 Where there is a complaint relating to the care of a patient, the patient must be made aware that staff who have not been involved in their care will have access to information contained within their health record.

Subject Access Requests

5.9 Patients are entitled to obtain a copy of their health record, and it is good practice for all staff to be open with patients about all information that is entered into their health record. Requests to access patient information from either patients, solicitors or others acting on behalf of patients must be passed to the health records department for handling under the Data Protection Subject Access Procedure.

5.10 There are situations where it is not reasonable to obtain consent for the use or disclosure of patient identifiable information. Where this is the case, Section 251 of the NHS Act 2006 provides authorisation to allow patient identifiable information to be disclosed without the consent of the patient e.g. clinical audit, record validation.

6. BREACHES OF CONFIDENTIALITY

6.1 All staff are strictly forbidden to access any personal information relating to relatives, friends or colleagues unless they have legitimate reason to do so as part of their employment responsibilities.

6.2 Breaches of confidentiality and near misses must be reported in accordance with the Management of Adverse Events Policy and Procedure, and where applicable, the Serious Incident Policy and Procedure. Breaches must also be reported to Caldicott Guardian.

6.3 Staff responsible for breaches of confidentiality will be dealt with according to the Disciplinary Policy and Procedure, which could result in summary dismissal or other action. Staff may also be subject to legal and / or civil action taken against

them.

7. STORAGE AND DESTRUCTION OF CONFIDENTIAL INFORMATION

7.1 Confidential information must be kept secure from unauthorised access

7.2 Paper-based confidential information should always be locked away when not in use, and preferably in a room that can be secured

7.3 Electronic-based confidential information should not be held on local hard drives (C: drives) but should be held on shared network drives with access limited to authorised staff, as per the Creation of Corporate Records Procedure and the Safe Haven Procedure.

7.4 CDs, memory sticks and other portable media containing confidential information must be encrypted and password protected, and should not be used for the permanent storage of confidential information, as per the Safe Haven Procedure.

7.5 It is vital confidential information is safeguarded at every stage and that the method used to destroy records is fully effective.

7.6 Staff must ensure that the patient information is sent securely e.g. using NHS Secure email, File Transfer, encryption tools or Safe Haven procedures

8. TRANSFERING CONFIDENTIAL INFORMATION

The Safe Haven Procedure acts as a safeguard for confidential information which enters or leaves the GP Care Group, whether this is by fax, e-mail, post or other means. Refer to the Safe Haven Procedure for details.

9. CONFIDENTIALITY OF PASSWORDS AND SMARTCARDS

9.1 Personal passwords issued to or created by staff should be regarded as confidential and those passwords should not be communicated to anyone else (refer to the Information Security Policy for further details).

9.2 Smartcards are issued to staff for their own use only. As per point 5 in the Smartcard National Terms & Conditions, Smartcards must not be shared, must not be left unattended nor the password communicated to anyone else.

10. DISSEMINATION OF DOCUMENT

Following approval by the Information Governance Committee, this policy will be submitted to the GP Care Group Board for ratification. It will then be uploaded onto the remote drive under Information Governance.

REFERENCES

References to Standards

- Information Governance Toolkit

Legislation

- Data Protection Act (1998).

Guidance

- Confidentiality: NHS Code of Practice (Nov 2003).