Confidentiality Code of Conduct for Employees

Author	Alyson Hope
Responsible Director	Medical Director
Ratified By	Quality and Safety Committee
Ratified Date	10 May 2012
Review Date	December 2015
Version	1.1
Policy Consultation Period	21.01.2015 – 20.02.2015

Related Policies & Guidelines:

- Safe Haven Policy
- Email and Internet Policy
- Information Security Policy
- Subject Access Request Policy

Please note that this document should be read and understood prior to the contract of employment or other confidentiality agreement being signed. If there is anything that is not clear please contact your manager.

Contents

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.1		December 2014	Review and formatting	Q&SC

1. Purpose of the Code

This Code of Practice details the required practice for those who work within or under contract to Central London Healthcare (CLH) to protect the security and confidentiality for all personally identifiable and confidential information. For the purposes of this document the terms “employee” or "staff" are used as a convenience to refer to all those to whom this code should apply. Whilst directed at Central London Healthcare’s staff it is also relevant to any one working in and around Central London Healthcare to include contractors, agency staff, students and volunteers.

This Code has been written to meet the requirements of:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988
- The Freedom of Information Act 2000
- The Access to Health Records Act 1990
- Confidentiality: NHS Code of Practice 2003
- Common Law Duty of Confidentiality

All employees working at Central London Healthcare are bound by a duty of confidence to protect personal information. This is a requirement established within Common Law. In addition, for clinical and other professional staff, it is contained within their own professional codes of conduct.

This means that all employees are obliged to keep any person-identifiable information secure and strictly confidential. This includes both patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should be also be treated with the same degree of care, e.g. business in confidence information such as patient referral letters, discharge summaries, waiting list data, consultants’ workloads, clinic lists.

The principle behind this Code of Conduct (The Code) is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of Central London Healthcare's security systems or controls in order to do so.

This Code has been produced to protect employees by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. Breach of confidentiality of information gained, either directly or indirectly, in the course of duty is a disciplinary offence that could result in dismissal, bring into question their professional registration and possibly result in legal proceedings against them.

2. Confidentiality

2.1 Duty of confidence

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician; colleague to colleague; employee to employer; commissioner to contractor) in circumstances where:

- it is reasonable to expect that information will be held in confidence
- it is a legal obligation that is derived from case law
- it is a requirement established within professional codes of conduct
- it must be included within NHS employment contracts as a requirement linked to disciplinary procedures

This can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends or organisational confidential information howsoever stored, whether on paper, floppy disc, CD, laptops, palmtops, mobile phones, tablets and digital cameras or by word of mouth.

This information can take many forms including medical notes, audits, computer files, employee records, occupational health records printout, video, photograph, etc.

Under the Data Protection Act 1998 information about a living person from which that person can be identified and which is held in either a manual or computer based filing system is protected. 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. A visual image (e.g. photograph) is sufficient to identify an individual.

For the purpose of the Data Protection Act 1998, information relating to the physical health, sexual life, racial or ethnic origin, or religion of a patient is deemed sensitive personal data requiring an added layer of protection.

In addition, certain categories of health information are further legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

Whilst working at CLH, employees should consider all information to be sensitive, even something as simple as a patient's name and address. The same standards should be applied to all information employees come into contact with.

2.2 Ensuring that the subject understands and consents to the use made of their information

In order to give their consent, staff and patients must understand and agree to how Central London Healthcare will use information about them. Central London Healthcare for its staff or the practitioner for the patients must discuss the uses of their information with them.

Leaflets are useful for reinforcing information given to a person, but are not in themselves sufficient. Any explanation should include as a minimum that:

- the main use of the information will be to manage the patient's care and treatment, and that it is very important that we have full and accurate information if we are to provide the best care.

- Central London Healthcare, or a regulatory authority, also uses their information to check the quality of the care that they and other patients receive, to ensure that this is of the right standard. This process is called audit. Everyone involved in audit has to follow the same strict rules on confidentiality.

- the staff work as part of a team and will share information about Central London Healthcare with the team if it is necessary to provide the best care for them. If the staff work with members of another agency then they should explain that information may be passed to that agency if it is necessary to provide their care, but that the agency has also signed up to the same standards of confidentiality.

- they have a right of access to their health records by making a subject access request in writing and that a leaflet is available if they wish to have more information on their right. Staff themselves should be familiar with the Subject Access Request Policy.

- we send anonymous information to the Department of Health or Central London Clinical Commissioning Group to allow us to manage the service and monitor its effectiveness.

2.3 Does the consent need to be in writing?

It is not usual practice to obtain written consent to the use of information for care and treatment. If in doubt, staff must seek advice from the Central London Healthcare's Caldicott Guardian.

2.4 What if patients do not consent?

If patients do not consent to our proposed use of their information then Central London Healthcare cannot use it in that way. It is important that patients fully understand the implications of such a decision and in serious situations where the well-being of the patient or others may be compromised the staff should seek advice from Central London Healthcare's Caldicott Guardian, and the senior practitioner responsible for the patient. Such a decision must be carefully documented and reported to the responsible practitioner.

2.5 Ensuring that the subject understands the limits of confidentiality

Staff should explain to the subject that in some circumstances they will be obliged to pass on or act upon information even if the subject objects. This will apply if a failure to pass on information may lead to harm to the patient or someone else. There are also certain legal requirements to pass on information that can be explained to the patient if required.

2.6 Collecting only what is necessary

Staff should only collect as much personal information as is necessary for the agreed purpose, and no more. The information collected must be adequate but not excessive. Most healthcare records are by necessity very detailed, but they must nevertheless be accurate and relevant. Employees should refer to Appendix 1 for more information on record keeping best practice.

Where information is extracted for other agreed purposes (for example audit) there should be a sound rationale for every piece of information that is used. Personal identifiers should be removed from the data if they are not strictly necessary for the intended use.

2.7 Recording the information accurately

Staff have a legal obligation to ensure that any personal information on file is accurate. If information is recorded inaccurately, future decisions may be wrong and harmful to the patient, result in delays or mislead research. Data is regarded as inaccurate if it is incorrect, misleading or out of date as to any matter of fact.

Subjects have a legal right to have inaccuracies of fact corrected or removed from record, and to have an entry made in their record if they disagree with a statement of opinion.

3. Requests for Information on Patients and Staff

All patients have the right under the Data Protection Act 1998 to see and/or have copies of the information Central London Healthcare holds about them. If a member of staff receives a request from a patient for access to their notes, please let the FOI Lead know and he/she will deal with it. Other members of staff are not authorised to deal with such requests. Details of how such requests are dealt with by Central London Healthcare are contained in the Subject Access Request Policy.

In relation to requests made by a person other than a patient:

- staff should never give out information on patients or staff to persons who do not “need to know” in order to provide health care and treatment
- all requests for identifiable information should be on a justified need and some may also need to be agreed by Central London Healthcare’s Caldicott Guardian

If the staff have any concerns about disclosing/sharing patient information the staff must discuss with their manager and if they are not available, someone with the same or similar responsibilities. If the staff cannot find anyone to discuss the issue with, they should wait until someone is available and only disclose when this has been discussed with a manager.

3.1 Telephone enquiries

If a request for information is made by telephone, staff should

- always check the identity of the caller and
- check whether they are entitled to the information they request
- take a number, verify it independently and call back if necessary

3.2 Requests for information from the Police and media

With respect to the Police

- Requests for information from the Police should always be referred to the Caldicott Guardian or the Head of Performance and Information.

With respect to the Media

- Staff should not give out any information under any circumstances. If a member of staff is contacted in person or by phone, he or she should refer the person to the Managing Director, who deals with all communications matters.

3.3 Abuse of privilege

It is strictly forbidden for staff to look at any information relating to their own family, friends or acquaintances unless they are directly involved in the patient's clinical care or with the employees administration on behalf of Central London Healthcare. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

If members of staff have concerns about this issue staff should discuss with their line manager.

3.4 Carelessness

Employees should:

- not talk about patients/patients in public places or where the staff can be overheard
- not leave any medical records or confidential information lying around unattended
- make sure that any computer screens, or other displays of information, cannot be seen by the general public

4. Transfer of Information (see also Safe Haven Policy)

4.1 Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

External mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as case notes, or collections of patient records on paper or memory stick. These should be sent by Recorded Delivery or by NHS courier to safeguard that these are only seen by the authorised recipient(s). The recipient of the mail should be asked to confirm receipt and, if this is not done, contact should be made to acknowledge delivery.

Electronic media should be password protected. Advice on how to password protect files is available from Central London Healthcare's Head of Performance and Information or the ICT Service Desk on 0203 350 4050.

4.2 Faxing

- Staff should remove patient identifiable data from any faxes unless the fax is sent to a known secure and private area (so-called Safe Havens).
- Faxes should always be addressed to named recipients.
- Staff should always check the number to avoid misdialling and ring the recipient to check that they have received the fax.
- If the fax machine stores numbers in memory, staff should always check that the number held is correct and current before sending sensitive information.
- All faxes should include the approved Central London Healthcare cover sheet which is clearly marked that the fax is STRICTLY CONFIDENTIAL. All faxes must contain the named recipient in the To: field.

4.3 Email

The email transmission of this information internally/externally over Central London Healthcare's network can pose serious risks to confidentiality, and should only be done when essential to the delivery of healthcare. All transmission of identifiable information should be in line with Central London Healthcare's Email and Internet Policy.

Patient identifiers should be removed wherever possible, and only the minimum necessary information sent. This may be considered to be the NHS number but no name or address although this in itself can pose problems as the wrong number may be typed.

Special care should be taken to ensure the information is sent only to recipients who need to know; always double check that staff are sending the email to the correct person(s).

External transfers should only take place to persons with access to NHS.net. Under no circumstances whatsoever should any type of patient identifiable information or sensitive or confidential information about any other person be e-mailed to persons who do not have a secure email. In addition to NHSmail, the following government domains are considered secure:

- GSi (*.gsi.gov.uk)
- GCSX (*.gcsx.gov.uk)
- CJX (*.police.uk or *.pnn.police.uk)
- SCN (*scn.gov.uk)
- GSE (*.gse.gov.uk)
- CJSM (*.cjsm.net)
- GSX (*.gsx.gov.uk)
- MoD (*.mod.uk)

Due to its insecure nature, any information transmitted over the Internet should be considered to be in the public domain.

Please refer to Central London Healthcare's Information Security policy and for more detailed information.

5. Storage and Confidential Information

Any paper-based confidential information (e.g. GUM records) should always be kept locked away and preferably in a room that is locked, and in some cases alarmed when unattended, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time.

Electronic patient information must not be saved onto local hard drives or onto removable media, but onto the Central London Healthcare's network. The only acceptable removable media for storing patient information is an encrypted memory stick. These are available, once the line manager has given authorisation, from the Systems Manager. No PC at Central London Healthcare is equipped with a floppy drive and CD drives are configured for read-only purposes.

Appendix 2 sets out in more details the requirements to keep patient information secure.

6. Disposal of Confidential Information

When disposing of **paper-based person-identifiable information** or confidential information employees should always use 'Confidential Waste' bins. Employees must keep the waste in a secure place until it can be collected for secure disposal.

Computer printouts should either be shredded or disposed of as paper-based confidential waste.

Floppy discs/CDs are not used by Central London Healthcare.

Computer hard disks are disposed of by IT CSU.

7. Confidentiality of Passwords

Personal passwords issued to or created by staff should be regarded as personal and confidential and:

- Should never be written down
- Should not relate too easily to the employee or the system being accessed
- Should be changed if no longer secret or the system prompts staff to do so

Staff are responsible and accountable for all activities carried out under their name. Staff should never allow others to use their passwords unless otherwise authorised in writing. Staff will be given

more information about password control and format etc. when they receive their training and/or password.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the Information Governance Lead and may result in a disciplinary action and also to a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 1998, which could lead to criminal action being taken.

8. Working at home with patient identifiable information

It is sometimes necessary for employees to work at home. If required, it is necessary first to gain approval from their line manager. If this is agreed, the member of staff will be provided with a Central London Healthcare laptop, which has been encrypted and configured so that no information or documents can be saved onto it. This laptop must be used to "dial in" to the Central London Healthcare network. It is not possible for a member of staff to use his/her own laptop or PC to dial into the Central London Healthcare network.

Any staff member working from home must not access patient identifiable information of any level.

If taking home computer records on a memory stick or any other removable media, staff must ensure that memory sticks are encrypted. In addition, if this information is saved onto their own PC, staff must ensure that the information is removed again when finished. Other family members must not be able to access this information.

9. Software

All computer software used within Central London Healthcare is regulated by licence agreements. A breach of the agreement could lead to legal action against Central London Healthcare and/or the offender (member of staff).

It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach of the licence agreement.

All Central London Healthcare's PCs have been configured so that members of staff do not have permission to download any personal software onto the Central London Healthcare network.

10. General Provisions

10.1 Interpretation

If any person requires an explanation concerning the interpretation or the relevance of this Code, they should discuss the matter with their line manager, the Head of Performance and Information or the Caldicott Guardian.

The provisions of this Code apply to employees during their relationship with Central London Healthcare and after the relationship ceases.

10.2 Non-compliance

Non-compliance with this Code by any person working for Central London Healthcare may result in disciplinary action being taken in accordance with Central London Healthcare's disciplinary procedure, and may lead to dismissal for gross misconduct.

To obtain a copy of the disciplinary procedures employees can ask their line manager.

10.3 Amendments

This Code will be amended as necessary to reflect Central London Healthcare's development of policies and procedures and the changing needs of the NHS.

11. Confidentiality Statement

All Central London Healthcare e-mails should contain the disclaimer as detailed below, along with the individual's work contact details.

The CLH e-mail service may only be used for the communication of NHS information in accordance with NHS Information Governance Codes of Practice.

This email is intended only for the use of the above named person or service. It may contain information that is privileged or confidential. If you are not the intended recipient, any dissemination, disclosure, or copying of this communication is prohibited. If you have received this in error, please notify the department as mentioned above immediately and delete the e-mail or destroy the fax either by shredding or incineration.

All Central London Healthcare faxes contain the disclaimer as detailed below:

The information contained in this fax is STRICTLY CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately. Thank You.

12. Monitoring

12.1 Monitoring of emails and telephone use

Central London Healthcare will not routinely monitor staff emails or telephone calls. Any monitoring of staff email would only be done in exceptional circumstances where there are reasonable grounds for suspecting gross misconduct on the part of a member or members of staff. The Managing Director's authorisation is required before any monitoring of email or telephone use may be carried out.

12.2 Monitoring of internet access

Members of staff should be aware that the internet sites and time spent on the internet may be monitored. NWLCSU, who host Central London Healthcare's network, maintains software to enable managers to do this where there is evidence of inappropriate or excessive use. For full details, please refer to the Email and Internet Policy.

Appendix 1 – Record keeping best practice

Patient records should:

Be factual, consistent and accurate

- be written as soon as possible after an event has occurred, providing current information on the care and condition of the patient;
- be written clearly, legibly and in such a manner that they cannot be erased;
- be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly;
- be accurately dated, timed and signed or otherwise identified, with the name of the author being printed alongside the first entry;
- be readable on any photocopies;
- be written, wherever applicable, with the involvement of the patient or carer;
- be clear, unambiguous, (preferably concise) and written in terms that the patient can understand. Abbreviations, if used, should follow common conventions;
- be consecutive;
- (for electronic records) use standard coding techniques and protocols;
- be written so as to be compliant with the Race Relations Act and the Disability Discrimination Act.

Be relevant and useful

- identify problems that have arisen and the action taken to rectify them;
- provide evidence of the care planned, the decisions made, the care delivered and the information shared;
- provide evidence of actions agreed with the patient (including consent to treatment and/or consent to disclose information).

And include

- medical observations: examinations, tests, diagnoses, prognoses, prescriptions and other treatments;
- relevant disclosures by the patient – pertinent to understanding cause or effecting cure/treatment;
- facts presented to the patient;
- correspondence from the patient or other parties.

Patient records should not include

- unnecessary abbreviations or jargon;
- meaningless phrases, irrelevant speculation or offensive subjective statements;
- Irrelevant personal opinions regarding the patient.

Appendix 2 – Keeping patient information secure

For all types of records, staff working in offices where records may be seen must:

- Shut/lock doors and cabinets as required.
- Wear building passes/ID if issued.
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- Not tell unauthorised personnel how the security systems operate.
- Not breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity – though not indicating the reason for sensitivity – and permitted access, and the availability of secure means of destruction, e.g. shredding, are essential.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children's or pet's names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver to prevent casual viewing of patient information by others.

Appendix 3 – References

NHS Confidentiality Code of Practice 2003
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

IT Acceptable Usage – ICT Department, Westminster PCT

The Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

The Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

The Computer Misuse Act 1990
http://www.legislation.gov.uk/ukpga/1990/18/contents

The Copyright Designs and Patents Act 1988
http://www.legislation.gov.uk/ukpga/1988/48/contents

The Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

The Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

Confidentiality: NHS Code of Practice 2003
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Common Law Duty of Confidentiality
http://www.dhsspsni.gov.uk/gmgr-annexe-c8