NHS
Wandsworth
Clinical Commissioning Group

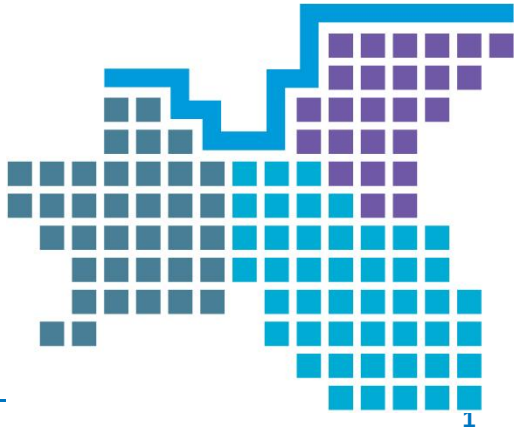
Confidentiality Code of Conduct

Mutiti Charity (WPCT)

Date for Review: 1 December 2017

Lead Director: Director of Performance, Quality and Corporate Affairs

NOTE: This is a CONTROLLED Document. Any documents appearing in paper form are not controlled and should be checked against the server file version prior to use.



DOCUMENT CONTROL AND AMENDMENT RECORD

Confidentiality Code of Conduct

Document Name:	Confidentiality Code of Conduct
Consultation:	SIRO &IGSG and IGC
Approved by:	IGSG & Integrated Governance Committee(IGC)
Description:	A code of conduct for the organisation, staff and those working on its behalf for the maintenance of confidentiality.
Audience:	All Staff
Contact details:	IG Manager
Supersedes	Confidentiality Code of Conduct 2012-2014

Change History

Version	Date	Author	Approver	Reason
0.1	Oct-14	IG manager		Initial Draft
0.2	Oct-14	SIRO		Review
0.3	Nov 2014	IG manager	IGSG	Approval
0.4	Dec-14	IG manager	IGC	Approval

CONTENTS

1. Introduction

This Confidentiality Code of Conduct has been produced to guide all Wandsworth Clinical Commissioning Group (WCCG) staff so that they are aware of their legal duty to maintain confidentiality. It outlines some guidance and standards that MUST be followed by all staff so as to protect personal and corporate confidential information.

Everyone working for WCCG is under a legal and contractual duty to keep personal information confidential. This duty also extends to corporate-confidential information where the legitimate business interests or operations of CCG could be damaged or hindered by unauthorised disclosure. Members of the public (including staff) who believe their confidence has been breached may make a complaint to WCCG and could take legal action against the organisation and/or individuals responsible for the breach.

This code of conduct applies to all staff (Including students, trainees on temporary placements, temporary staff, lay members and volunteers) who hold, obtain, record, use, store, share or destroy patient, employee or corporate confidential information. Information obtained from a patient or staff member directly, or about them for any other source, whether written, verbal or transmitted by or held on computer is covered by the Code of Conduct. The code also applies to all staff mentioned above even when not working for WCCG no matter how much time passes.

2. What is Confidential Information

Confidential information is of two main types:

2.1 Personal Information

Personal Information is any information if either on its own or combined with other information can lead to identification of an individual. It is of two main types - **Personal Identifiable** (referred to within the DPA as 'personal data') and **Personal Sensitive** (referred to in the DPA as 'sensitive personal data') as below.

Personal Identifiable – e.g. Name, address, date of birth, NHS Number, visual image. (See also Caldicott review 2 for an additional list of identifiable items)

Personal Sensitive – e.g. racial/ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, offences-committed or alleged, details of proceedings of offences

Note- this definition of personal data is based on the DPA 1998, however although the Data Protection Act 1998 is only relevant to the personal information of living individuals, this code also covers information about deceased service users

2.2 Corporate-Confidential Information

Any information which is defined as such by WCCG and which has not already been made available to the public, is essential to the core function of the organisation, and, if available in the wrong hands, may cause reputational damage.

Consideration as to confidentiality must also be given to similar information received from third parties.

Corporate-confidential information includes but is not limited to business strategies and plans (both final and draft), operational budgets, quotes, tenders, contracts, legal advice and investigations, 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.

3. Confidentiality Guidelines and Standards

All staff are expected to follow the following guidelines and standards;

3.1 Requests for information on patients

- Never give out information on patients to persons who do not "need to know" unless there is a legal basis(such as consent, court order or other legal powers)
- If it has been determined information should be disclosed, ensure only the minimum information is disclosed, not the whole record, unless there is a justification to do so.
- All requests for identifiable information should be on a justified need and in some cases may also need to be agreed by the Caldicott Guardian and/or the Information Governance Manager, to ensure protocols are being followed. If you have any concerns about disclosing/sharing personal information you must discuss with your manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with you should take down the callers details and ring them back when you are satisfied the disclosure of information can take place.

3.2 Disclosure of information to other WCCG employees

Information on patients should only be released on a need-to-know basis. Staff must:

- Always check the member of staff is who they say they are, by checking the employee's ID badge and/or their internal extension number or bleep number prior to giving them any information
- Use reasonable means to check with managers whether they are entitled to the information
- Not be bullied into giving out information inappropriately.

3.3 Requests for information by the media

Staff contacted by the media must not give out any information under any circumstances, and must refer enquiries to the communications team in the CSU.

3.4 Phone use (mobile or landline)

When receiving calls requesting personal information:

- verify the identity of the caller
- ask for a reason for the request

- If in doubt as to whether information should be disclosed tell the caller you will call them back. Take advice from your manager, and call back to main switchboard or known and trusted numbers only if possible
- Conduct conversations involving personal identifiable/ sensitive information in a secure manner where it cannot be overheard by unauthorised individuals e.g. in a private room or by lowering voice, avoid doing so in public areas such as when on public transport or supermarkets.
- Avoid leaving messages where possible or discourage others from leaving a voicemail on your phone with confidential information if phone not security coded
- Where possible, use passwords to gain access to answer phones for recorded telephone messages
- If messages are received via voicemail - they are to be deleted as soon as no longer needed
- Ensure messages cannot be overheard whilst being played back
- Staff must never send confidential information by text message
- No pictures of any confidential information are to be taken with mobile camera phones
- If your mobile phone is lost or stolen, it needs to be reported immediately to ICT, so appropriate action is taken to ensure no unauthorised access to the messages on the phone (see also section 3.12)

3.5 Use of internal and external post

All correspondence containing personal information should be addressed to a named recipient e.g. to a person, a post holder, 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. 'Private and Confidential' or 'Addressee Only', as appropriate.
- **External mail** - staff should consult IG manager for the best method to use due to the constantly changing secure postage/transportation methods. Common ones are special delivery (signed for), via CCG contracted courier. Special care is a MUST with personal information sent in quantity such as case notes, or collections of records on paper with personal information, CD or other media.

3.6 Faxing

When sending a fax:

- Avoid faxing personal or confidential information unless it is absolutely necessary
- If it is necessary, ensure that you fax the information to a Safe Haven fax (details of safe have are in the information life Cycle management protocol)
- Confirm the fax number
- Ask the recipient to confirm receipt of the fax
- Ensure you mark the fax header "Private and Confidential"
- Where possible personal details (e.g. name & address) should be faxed separately from clinical details, which must be accompanied by the NHS Number

- Where e-faxes are used staff should ensure the appropriate privacy impact assessment have been carried out if the service if from a third party organisation

When receiving a fax:

- Make sure you receive your faxes to a safe haven fax. Staff are responsible for familiarising themselves with where these are located in their work areas if available
- Always check your fax to make sure no faxes are left lying around, and
- Where possible advise to not have faxes sent to you in your absence.

3.7 Storage of confidential information

- Keep non-computerised confidential information where others cannot see it
- Ensure that filing cabinets containing confidential information are kept locked when not in use
- Ensure filing cabinets are not in areas which are accessible to members of the public/visitors
- Ensure regular housekeeping of your files, and
- When destroying information ensure you comply with records retention schedules and disposed in confidentiality bins
- Storage of all electronic information should be on CCG allocated folders on shared and personal drives only (this is a MUST even when working remotely (see section 3.12). CCG issued USB sticks may be used as a temporary storage (see also section 3.12)

3.8 Disposal of confidential information

- All confidential Information(paper based) must be disposed in 'Confidential Waste bins
- Inform relevant authorities when Confidential Waste bins are full – Do not use when full (Keep the waste in a secure place until it can be collected for secure disposal).
- Confidential waste paper must not be used as scrap paper for messages, notes etc.
- Staff are responsible for familiarising themselves with where these are located in their work areas.
- Computer hard disks are disposed of securely by the ICT team. For further information please contact the ICT Service Desk.

3.9 Passwords

- Never write passwords on paper
- Create one with a mixture of alphanumeric, letters and characters
- Do not share passwords; this may lead to disciplinary procedures
- Change password regularly; most systems will force a regular change of password and designate the format of it.
- 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 Manager, Caldicott Guardian or SIRO and may result in a disciplinary action. Staff should be aware that in some circumstances legal action may be taken against individuals in breach of law and/or policy.

3.10 Emailing confidential information

- Special care should be taken to ensure the information is sent only to recipients who have a "need to know ". Staff must always check that they are sending mail to the correct person(s).
- Confidential information should only be emailed using a secure NHS.net account.
- There are some domains that are permitted to send confidential or sensitive information outside the NHS as they are secure with the NHS.net. The following list of email extensions sets out those secure e-mail systems so far that it is permissible to send to: *.gsi.gov.uk, *.gsx.gov.uk, *.cjsm.net *gcsx.gov, *.gse.gov.uk, *.pnn.police.uk, *.scn.gov.uk, *.cjsm.net, *.mod.gov.uk

Note: Some public organisations still allow sending email with confidential information by 'encrypting and password protecting the file of personal information and ensuring no other personal information or the password are sent in the same email and sending that through the normal domains that are not listed above'. Staff should be aware that this is not WCCG policy and therefore must not do this but it is acceptable to receive as such from outside organisations and continue to communicate via our NHS.net email

3.11 Office environment

- Remember to lock and secure the office when it is unattended and at the end of the day
- Whenever possible escort visitors at all times on site
- Staff must wear their identity badge at all times
- Operate a clear desk policy, especially when using a hot desk or working in an open plan office
- Do not leave confidential information unattended or on your desk overnight
- Be careful where you site your computer screen: ensure any confidential or personal information cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access, and
- Remember to log off your computer when leaving the office, or lock it for short absences.

3.12 Agile/remote/home working

Various media are used to support agile/remote/home working. These include, but are not limited to:

- Laptops
- Blackberries
- Mobile phones
- USB sticks
- Removable hard drives
- SIM cards
- Memory cards.

- Tablets
- Smartphones
- Home desktop

(For other technical guidance on use of removable media (especially where used to support agile/home working) please see the agile working policy)

The following are your Do's and Don'ts to be followed when agile/remote or home working:

- DO NOT Use your home computer to store Organisation information. Work directly from the Organisation's server and save documents on the CCG network drives via CITRIX OR a CCG issued encrypted USB data stick OR on the ONE drive/Team Sites from office 365.
- Report lost or stolen device straight away even your own device if used for work purposes
- Make sure you know how to **wipe/delete** data from your own device if it is lost/stolen so work related information is not at risk of being in the public. The CCG can provide this guidance too where appropriate but staff have to make sure they know who can provide them this assistance (from the manufacturer e.g. Apple, Android) especially for devices such as tablets, smartphones etc.
- Take copies of paper files or electronic documents home, rather than originals unless there is no alternative and only if necessary. The 'original' or 'master' copy of the information should be stored at the CCG and not at home,
- If original files are taken home, or to other establishments, ensure that this is recorded in the department/service area.
- Do not leave CCG information data or electronic media in unattended vehicles, even if locked in the boot
- Print only the minimum required to undertake work activity
- Do not leave paper or electronic files where they could be accidentally viewed by others, including family members
- Take all reasonable steps to maintain security of and prevent loss or damage to any data and/or records taken away from the Organisation
- Take reasonable measures to protect work related information at home from unauthorised access, amendment or loss(This includes access by family members)
- Consider what practical measures are needed to ensure the home environment is secure, i.e. not leaving papers in household areas where disclosures can take place.
- Take precautions against theft and loss, particularly on the journeys to and from work.
- Dispose of all confidential papers files in the CCG confidential bins at CCG premises only not at Home or in transit.
- Keep paper records separate from equipment and technology (because of the risk of theft) they must be carried in separate bags.
- Assess the risk involved with the loss of personal and business sensitive data, by addressing the following questions:
    - How serious would the consequences be if someone gained unauthorised access to this information?
    - How likely it is that someone could gain access to this information?
    - What security procedures and measures are in place and are they appropriate?
    - What is the cost of implementing appropriate security procedures and measures?
- Do not use a personal e-mail account for Organisation business or vice-versa. If you have to use your Organisation email account for personal business please keep separately and store separately to avoid possible problems with DPA or FOI requests

- Use CCG and/orNHS.net e-mail accounts for work and personal email accounts for personal use only – avoid mixing the two.
- Keep home computer systems and applications virus protected and up-to-date
- Make use of security features such as encryption and password protection.
- Any person confidential data or corporate confidential data transferred to an encrypted USB data stick must:
    - be a copy of what is on your secure network drive;
    - remain encrypted and must not be transferred to any other external system, e.g. a home or other computer;
    - be worked on by opening and saving changes back to the USB data stick;
    - be returned to the appropriate location, as an updated version of the file/s on your organisation network drive and deleted from the memory stick after the work required is completed.
- CCG staff should only use CCG issued USB sticks or check with IT if their own stick is compatible with CCG standards. (The CCG allows use of foreign USB sticks from visitors only and these will only have read only permissions)

3.13 Use of electronic recording devices

Electronic recording devices MUST not be used to record on CCG premises especially where CCG related matters are being discussed without the explicit **consent** of the individual's concerned, senior manager and/or organisation. This includes;

- Use of body worn video and /or recording equipment
- Camera phone or other devices that could be used to capture information during CCG business hours either on location or off location.

3.14 Abuse of privilege

It is strictly forbidden for employees 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 the organisation. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

3.15 Information incident reporting

All information-related incidents need to be reported, however minor. The purpose of the reporting is to identify potential problem areas and try to reduce the risk of these occurrences happening in the future. Make sure you are familiar with how to report incidents and if not sure ask your manager

3.16 Training

It is mandatory that all staff undertake Information Governance training as part of induction and on an annual basis.

4. Caldicott Principles

The Caldicott Principles apply to all patient information held within health and social care organisations. Some organisations who provide a service to patients are also complying with these guidelines as it is seen to be 'good practice'. Further

information relating to Caldicott can be obtained from the Caldicott Guardian as mentioned above.

The seven Caldicott principles state that staff should:

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Ensure whatever you do with patient information is always based on a justified 'need to know'. The confidentiality best practice guidelines provides detailed advice of what you should do whilst working within WCCG. Ensure you ask you manager if you are unsure of any of these requirements.

5. Other relevant policies

A full list of guidelines, evidence and references will be provided and maintained in the **Information Governance Framework**.

The WCCG will take actions as necessary to comply with all legal and professional obligations in particular those contained in:

Legislative and Regulatory Environment

- Data Protection Act 1998

- Freedom of Information Act 2000
- Human Rights Act 1998
- The common law duty of confidentiality.

Best Practice Standards

- HSCIC Guide to confidentiality
- DH Confidentiality NHS Code of Practice
- DH Information Security NHS Code of Practice
- NIGB The Care Record Guarantee
- DH The NHS Constitution
- Caldicott Review 2 2013
- HSCIC – A Guide to Confidentiality in Health and Social Care 2013

Other References

- NIGB The Care Record Guarantee
- DH The NHS Constitution