Central London Community Healthcare NHS
NHS Trust

Barnet ▮ Hammersmith and Fulham ▮ Kensington and Chelsea ▮ Westminster

Information Governance
6th Floor
64 Victoria Street
London
SW1E 6QP
Tel: 020 7798 1323
Web: www.clch.nhs.uk
Email: foi.request@clch.nhs.uk

Susan Davis via email to:
request-154391-a7c302d9@whatdotheyknow.com
Our ref: FOI/2013/029

8 May 2013

Dear Ms Davis

Freedom of Information Act 2000 request: *Hospital Chaplaincy Procedures*

With reference to your request for information, dated 24 March, made under section 1(1) of the Freedom of Information Act, I am writing to inform you that the information you require exists and is held by Central London Community Healthcare NHS Trust (CLCH). Please accept my apologies for the delay in providing you with a response.

You asked the following:

"1. tell me whether policies or procedures exist to:
a. establish whether a patient admitted to any of your hospitals does or does not wish to receive contact from a hospital chaplain"

Patients in the Trust's bedded services are given the choice to have contact with a chaplain if they wish. The Trust provides patients with details of how to access a chaplain of their chosen faith.

"b. ensure that patients (or their visitors, next-of-kin etc.) do not received unsolicited contact from chaplains"

Chaplains do not have access to patient information or details about visitors (including family and/or next of kin). If consent was received to disclose such information, the Trust would oblige within the limits of that authority.

"c. safeguard patients' personal and medical data such that hospital chaplains by default do not have access to it" and ***"d. ensure that hospital chaplains, when given access to patient data, do not share any of it with third parties"***

The Trust's *Confidentiality Code of Conduct* outlines the legal and contractual requirements placed on staff in relation to confidentiality to ensure that staff do not inadvertently breach any legal requirements.

All staff have a responsibility to ensure that personal information is handled appropriately and securely, and that adequate security provisions are implemented around such data to reduce the risk of a breach of the Data Protection Act (DPA) 1998.

"If you answered yes to any of the above, please could you provide me with copies of the relevant policies or procedures

A copy of the Trust's *Confidentiality Code of Conduct* is attached.

2. outline your approach for monitoring adherence to the policies and procedures above"

The Trust's Information Governance Group monitors adherence to the *Confidentiality Code of Conduct* and all related policies, which includes reviewing reported incidents and complaints logged in the Trust's incident reporting system.

The Trust is required to review Information Governance policy as part of its annual NHS Information Governance Toolkit submission. This is an online system which allows NHS organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations' IG Toolkit assessments.

"3. provide me with a summary of the results of this monitoring for the last five years, including rates of compliance with the policies and procedures, and severity of any non-compliance events"

The Trust's Information Governance Toolkit submission for the last year (2012/13) reports that the Trust is compliant with the required confidentiality and data protection assurances (set out in the 9 related requirements).

There have been no complaints or incidents logged relating to chaplaincy services since the Trust was formed on 1 November 2010.

The Toolkit can be accessed at https://www.igt.connectingforhealth.nhs.uk/ and you can search for CLCH's previous submission in the *Just Browsing?* section under organisation code *RYX*.

"4. provide me with details of any action taken in respect of any non-compliance identified (e.g. tightening of procedures, disciplinary action – in the latter case, taking care not to disclose any personal information)"

This information does not exist and hence is not held – there have been no such non-compliance incidents.

This completes our response to your request for information. I have also attached a copy of the template response which you asked us to complete.

If you are unhappy with our response, please write to us giving your reasons and we will address them. If you remain dissatisfied you are entitled to appeal to the Information Commissioner:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 113
Web: www.ico.gov.uk/complaints.aspx

Yours sincerely

S. Allison

James Allison
Information Governance Facilitator
Central London Community Healthcare NHS Trust

Central London Community Healthcare NHS
NHS Trust

Barnet ▮ Hammersmith and Fulham ▮ Kensington and Chelsea ▮ Westminster

Confidentiality Code of Conduct

Author(s):	Information Governance Facilitator Head of Information Governance & Management
Supporting Committee:	Information Governance Group
Policy No.:	**INFO07**
Version No.:	1
Validity Period:	October 2010 to October 2013
Target Audience:	All Staff

Table of Contents

1. Introduction

1.1. All employees of Central London Community Healthcare NHS Trust (CLCH) are bound by a legal duty of confidence to maintain the confidentiality and security of personal and / or confidential information. This is not just a key requirement of the Data Protection Act 1998, but is also a contractual obligation as an NHS employee.

1.2. A duty of confidence arises when one person discloses information to another e.g. patient to clinician, in circumstances where it is reasonable to expect that the information will be held in confidence; a principle which applies to all CLCH staff.

1.3. Personal information should only be disclosed with the consent of the individual concerned or where there is a robust legal justification / exemption to do so.

1.4. This Code of Conduct has been developed in line with the NHS Code of Practice on Confidentiality and outlines the responsibilities of all staff whilst providing them with guidance on how to ensure confidentiality is upheld. It has also been written to meet the following legal requirements;

- Data Protection Act 1998
- Computer Misuse Act 1990
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Caldicott Principles

1.5. The principle behind this Code is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.

2. Purpose and Objectives

2.1. The purpose of this Code is to outline the legal and contractual requirements placed on CLCH staff in relation to confidentiality.

2.2. By making staff aware of these responsibilities, CLCH aims to protect staff so that they do not inadvertently breach any of the legal requirements.

3. Scope

3.1. This Code applies to all staff employed by CLCH and / or with a responsibility for CLCH data, which may include contractors or staff employed by other organisations but working on behalf of CLCH. All staff are responsible for ensuring that confidentiality of CLCH data is maintained at all times.

3.2. This Code covers all sites, systems, personal and / or confidential information operated and utilised by CLCH held in both electronic and manual format.

3.3. Any breach of the NHS Code of Practice on Confidentiality (2003) or the Trust Confidentiality Code of Conduct will be considered an offence and CLCH disciplinary procedures will apply.

3.4. Any external agencies or organisations working with the Trust who have access to personal or confidential information will be expected to read and comply with this Code of Conduct. It is expected that departments / sections of the Trust who deal with such representatives will take responsibility for ensuring that those bodies have agreed to abide by this Code of Conduct.

4. Definitions

4.1. **Confidential information** is any information, both personal and non-personal, that when provided, was done so in the expectation that it would not be disclosed without relevant authority. It can be anything that relates to patients, staff, their family and friends and also to Trust information that is exempt from disclosure under the Freedom of Information Act 2000 (FOI). This class of information may be stored in any manner e.g. on paper, electronically, and could be stored on any device including, but not limited to, laptops; mobile phones; digital cameras; and USB memory sticks. Confidential information may also be passed by word of mouth.

4.2. **Data Sharing** is the disclosure of information from one or more organisations to a third party organisation (or organisations), or the sharing of data between different parts of an organisation. For example, several organisations pooling information or 'one off' disclosures in an emergency situation.

4.3. **Explicit consent** means articulated patient agreement. The terms relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

4.4. **Implied consent** means patient agreement that has been signalled by behaviour of an informed patient, for example, holding an arm out to allow the health professional to take blood.

4.5. **Information Commissioner's Office (ICO)** is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals."

4.6. **Personal data, otherwise known as person-identifiable data (PID),** is information which can identify a person from that data or part of that data. It includes any expression of opinion about any person. Personal information includes name, address, date of birth, or any unique identifier such as NHS number, RiO number etc. It also includes information which,

when presented in combination, may identify an individual, e.g. postcode, date of birth etc.

4.7. **Sensitive personal data** is information regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sexual orientation, criminal proceedings or convictions. These data are subject to more stringent conditions on their processing when compared to personal information.

5. Duties

5.1. Overall responsibility for the confidentiality and security of CLCH patient and staff information lies with the **Chief Executive.**

5.2. **The Head of Information Governance and Management** is responsible for ensuring compliance with the Data Protection Act 1998 and in particular the rights of data subjects such as patients and staff. They will also ensure adequate training and support around confidentiality and monitor the effectiveness of its implementation.

5.3. **The Caldicott Guardian** is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian also represents confidentiality issues at Board / Senior Management team level and is the Director of Medicine.

5.4. **The Senior Information Risk Owner (SIRO)** takes ownership for the organisation's information risk policy and acts as an advocate for information risk on the Board. The SIRO is the Director of Nursing Quality and IMT.

5.5. **All staff** have a duty to safeguard the confidentiality and security of personal information. This is governed by law, contracts of employment, professional codes of conduct and national requirements.

6. Legal and Professional Obligations

6.1. There is a wide range of legislation and guidance that relates to the use and disclosure of personal and / or confidential information including but not limited to:

Data Protection Act (DPA) 1998

6.2. The DPA reveals the legal provisions around processing personal data of living individuals. The term 'processing' includes any action related to the data such as obtaining, viewing, recording and disclosing. The Act applies to staff and patient records as well as paper and electronic records. At the heart of the DPA are the following 8 principles:

- Data shall be processed fairly and lawfully.
- Data shall be processed only for specified purposes.
- Data shall be adequate, relevant and not excessive.
- Data shall be accurate and kept up-to-date.
- Data shall not be kept for longer than necessary.
- Data shall be processed in accordance with individual's rights.
- Data shall be kept secure.
- Data shall not be transferred outside the European Economic Area (EEA) without adequate protection.

6.3. The Act allows for third party access to personal information e.g. Police, Local Authorities. This is only under certain circumstances known as exemptions. Staff should contact the IG team or Caldicott Guardian in such cases.

Freedom of Information (FOI) Act 2000

6.4. This Act legislates the general public's right to access non-personal information held by public authorities. The principles of openness and transparency are key principles behind this Act.

6.5. Non-personal, non-confidential information relating to CLCH and its services will be available through a variety of media as detailed in the Trust's Freedom of Information Publication Scheme.

Human Rights Act 1998

6.6. Article 8 of the Human Rights Act 1998 establishes a right to 'respect the private and family life'. This identifies a duty to protect the privacy of individuals and preserve the confidentiality of their health records. Compliance with the DPA ensures the Trust is meeting its obligations under Human Rights legislation.

Crime and Disorder Act 1998

6.7. The Crime and Disorder Act provides the power to disclose information to the Police for the purposes of preventing or detecting crime. It does not provide a duty to disclose, and does not override a healthcare professional's Common Law Duty of Confidentiality.

Computer Misuse Act 1990

6.8. The Computer Misuse Act makes it an offence to access information held within a computer system without authority. Staff therefore must only access information that they are authorised to access and not share this access with others (by allowing others to use their user login and password). Staff must not alter information where they are not authorised to do so.

6.9. The Computer Misuse Act creates three specific offences:

- Unauthorised access to computer material
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a crime
- Unauthorised modification of computer material

6.10. The Trust will undertake or commission regular audits to assess its compliance with legal requirements.

Common Law Duty of Confidentiality

6.11. Common Law is a form of law based on previous court cases decided by judges. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

6.12. In practice, this means that all personal information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. However, there are some legal exemptions that permit the disclosure of personal information, this is discussed further in section 8.

Caldicott Principles 1998

6.13. The Caldicott Principles are a set of guidelines developed specifically for handling Patient Identifiable Information (PII). The Director of Clinical Leadership, Quality and Safety and IM&T is the appointed Caldicott Guardian within CLCH. This role governs the ways in which personal information is managed.

6.14. The 6 Caldicott principles are:

- Justify the purpose for using PII
- Only use PII when absolutely necessary
- Only use the minimum PII necessary

- Access to PII should be on a strict need-to-know basis
- Everyone must be aware of their responsibilities when handling PII
- Understand and comply with the law

Professional Code of Conduct

6.15. All staff working for or on behalf of the NHS have an obligation to adhere to the required standards of practice in the 'Confidentiality: NHS Code of Practice'.

6.16. This Code of Practice is based on legal requirements and best practice concerning confidentiality and patients' consent. The Code offers detailed guidance on:

- Protecting personal and / or sensitive, confidential information
- Informing patients about uses of their personal information
- Offering patients appropriate choices about the uses of their personal information
- The circumstances in which confidential information may be used or disclosed. The document can be accessed via the connecting for health website (www.connectingforhealth.nhs.uk)

6.17. This Code of Practice should be adhered to in line with Professional Codes of Practice such as Medical Royal Colleges Codes, The Nursing and Midwifery Council, General Medical Council, British Medical Association etc.

Contractual Code of Conduct

6.18. Staff have a contractual obligation to maintain confidentiality of personal and / or sensitive information; particular attention is drawn to the following:

- Information regarding service users must not be disclosed either verbally or in writing to unauthorised persons. It is particularly important that staff ensure the authenticity of telephone enquiries
- Written records, computer records and correspondence pertaining to any aspect of the organisation's activities must be kept securely at all times
- Staff have an obligation to ensure that computer systems which they use are protected from inappropriate access within their direct area of practice e.g. by ensuring that passwords are kept secure, including smartcards and ID cards.
- All data held, its management and procedures must conform to the requirements of the Data Protection Act (1998). Under the Act, service users and staff have a right of access to their records.
- If it is necessary for staff to share information in order to effectively carry out their duties, they must ensure that as far as is reasonable that the information will be exchanged on a strictly 'need to know' basis, using the minimum data that is required and be used only for the purpose for which the information was given.
- Staff should seek advice from the Trust's Caldicott Guardian or IG Team where they are unsure.
- Conversations relating to confidential matters affecting clients should not take place in situations where they may be overheard by passers-by, e.g. in corridors, reception areas and lifts.
- The same confidentiality must also be observed in dealing with work related matters concerning work colleagues.
- Any breach of confidentiality may be regarded as misconduct and may be subject to disciplinary action and legal proceedings.

Confidentiality

7. Principles of Confidentiality

7.1. All staff have a responsibility to ensure personal and / or sensitive information is handled appropriately and securely. Adequate security provisions must be implemented around such data to reduce the risk of a data loss incident or breach of the Data Protection Act (DPA) 1998.

7.2. Staff should refer to the Transfer of Personal Information Code and the Information Security Code for further guidance however, some key information security provisions to apply are;

- Ensure passwords are a minimum of six characters and contain both letters and numbers.
- Lock computers / workstations when away from leaving desks unattended (ctrl+alt+del).
- Lock filing cabinets and rooms when not in use.
- Do not share security passes, passwords or smartcards.
- Discuss confidential conversations in private.
- Use NHS mail to transfer personal and / or confidential data.
- Do not leave laptops / files in unattended vehicles or easily accessible areas.
- Avoid removing personal information such as patient records unless previously agreed by the Caldicott Guardian.
- Send fax messages to safe haven fax machines and confirm receipt of fax.

7.3. Staff must ensure that patients within their care are kept fully informed about the purposes for which information about them is collected and used. This can be achieved by checking whether service users have seen available information leaflets or posters, whilst making it clear when

information is recorded or health records are accessed, e.g. *'I am just taking a note of your blood pressure'*.

8. Confidentiality of Patient Information

8.1. The confidentiality of patient information must be maintained at all appropriate times. This can be achieved by aspects such as not discussing outside work purposes, taking care when discussing cases, keeping information physically and electronically secure and only disclosing information in line with the Caldicott and Data Protection principles.

8.2. Information should only be accessible to those authorised. Staff may only access information that is relevant to their role and directly involved with the care of individual patients. Staff must not deliberately access their own clinical or HR records, either manual or electronic, or the records of relatives or friends unless this is done through a formal subject access request: *see INFO05 Access to Health and Personnel Records Code*.

8.3. The transfer of patient identifiable information must satisfy Caldicott principles and receive Caldicott approval. *See Transfer of Personal Information Policy*.

8.4. However, it is also important that confidentiality does not obstruct the provision of care. Under the DPA, there are provisions and exemptions that permit the exchange of person-identifiable information without the consent of the individual, particularly where it is necessary for the efficient and effective operation of the Trust and its partner organisations.

8.5. Staff should consult with a member of the IG Team or Caldicott Guardian in such cases.

9. Confidentiality of Children and young people's information

9.1. Once children reach the age of 16, they are presumed in law to receive the same duty of confidentiality as adults. This means that in many respects they should be treated as adults – for example, if a signature on a consent form is necessary, they can sign for themselves.

9.2. However, it is still good practice to encourage competent children to involve their families in decision-making. Where a competent child does ask you to keep their confidence, you must do so, unless you can justify disclosure on the grounds that you have reasonable cause to suspect that the child is suffering, or is likely to suffer, significant harm.

9.3. In regards to children under the age of 16, they need to be deemed 'Fraser competent' (also known as Gillick competent). This means that "the parental right to determine whether or not their minor child below the age of 16 will have medical treatment terminates if and when the child achieves sufficient understanding and intelligence to enable him / her to understand fully what is proposed".

9.4. The Data Protection Order 2000 (Subject Access Modification) ruled that where information has been provided by a child in the expectation that it would not be disclosed to their parent / guardian, or where it has been obtained as a result of any investigation to which the child consented in the expectation that it would not be disclosed, neither parents nor guardians have an automatic right of access where a child has been deemed 'Fraser competent' and is aged 12 or over.

9.5. You should never automatically assume that a child with learning / mental difficulties is not competent to make his or her own decisions. In most cases, children will be competent if information is presented in an appropriate way and they are supported through the decision-making process.

9.6. If a child who is under 16 does not have the capacity to consent, someone with parental responsibility can consent for them.

9.7. If a child of 16 and 17 is not competent to take a particular decision, then a person with parental responsibility can take that decision for them, although the child should still be involved as much as possible. Once children reach the age of 18, no one else can take decisions on their behalf.

9.8. The table below provides a list of people who can hold parental responsibility:

Child's mother
Child's father - If he was married to the mother when the child was born
For children born before 1 December 2003 - The child's father, if he marries the mother, obtains a parental responsibility order from the court or registers a parental responsibility agreement with the court
For children born on or after December 1, 2003 - The child's father, if he registered the child's birth with the mother at the time of the birth, or if he re-registers the birth (if he is the natural father), marries the mother, obtains a parental responsibility order from the court, or registers a parental responsibility with the court
Child's legally appointed guardian
A person with a residence order concerning the child
A local authority that is designated to care for the child
A local authority or person with an emergency protection order for the child
**Please note that the relevant paperwork would need to be produced in all cases as proof of parental responsibility*

10. Confidentiality of Staff Information

10.1. The confidentiality of staff information should be managed with the same regard as patient information and falls subject to the DPA, i.e. employee information can only be disclosed in line with legal requirements and exemptions.

10.2. Confidential information relating to employees must be provided with the same degree of protection as that afforded to patient information.

Information Sharing

11. Information Sharing

11.1. Information Sharing is essential in order to provide a better, more efficient healthcare service to patients.

11.2. There are two main types of data sharing;

- Systematic routine data sharing where the same data sets are shared between the same organisations for an established purpose
- Exceptional, one-off decisions to share data for any range of purposes.

11.3. A common misconception related to data sharing of personal information is that such data can automatically be shared with colleagues within CLCH as well as other NHS employees; this is not the case.

11.4. The legal requirements around the data sharing of personal information apply in all cases irrespective of the recipient. For this reason, CLCH requires all disclosures of personal and / or sensitive information to receive Caldicott approval to ensure this is shared in line with the DPA.

12. The Prison Environment

12.1. Maintaining confidentiality is particularly difficult in a prison. Prisons are closed societies and non-healthcare staff and inmates alike may discover something about a patient's health simply by observing which professional a prisoner is going to see or which drug is taken. Consequently, staff need to take extreme care to safeguard patient confidentiality.

12.2. There are occasions when it is essential to share information in a prison, such as:

- Giving information and advice to non-healthcare staff (wing manager, personal officers, teachers, workshop supervisors) about the best way to manage and support a particular patient on ordinary location.

- Participating in the multidisciplinary processes set up to plan the patient's sentence and then resettlement care in prison and back to the community. In some ways, this is comparable to participating in multidisciplinary Care Programme Approach (CPA) meetings in the community. It is essential to share information outside healthcare to facilitate creative solutions such as moves between wings and the healthcare centre, 'respite' stays in the healthcare centre, a mixed location (eg education centre or sheltered work during the day, the healthcare centre at night) and a planned response to a crisis, eg in the case of chronic self-injury in the presence of personality disorder, where several disciplines may be involved.

- Participating in procedures to support the multidisciplinary care of patients thought to be at risk of suicide or self-harm (currently in England and Wales - ACCT). Healthcare staff must provide clear guidance to other staff about the most effective ways of managing risk factors and what signs or symptoms should trigger a request for a further healthcare intervention.

- When the healthcare worker becomes aware that the patient presents a risk of serious harm to some other individual or group of individuals.

- Inmate medical records should be made available to a visiting doctor on a confidential doctor to doctor basis. In the case of a visiting psychiatrist, providing an opinion in relation to a possible admission to hospital under the Mental Health Act 1983, the right to access to the prisoner’s Inmate Medical Record is specifically referred to in the Mental Health Act Code of Practice.

12.3. It is also ethically correct for a medical officer to provide a report containing relevant medical information on a prisoner to the Local Review Committee / Board providing the following considerations are observed:

- The prisoner should first be seen by the health professional and advised that, for the purpose of consideration for parole, a medical

report has been requested. For the most part, prisoners are likely to give their consent to this as they will see it to be in their best interest. If the prisoner withholds consent, the medical officer's report should say so and it must not contain any fact or opinion based upon information obtained by the medical officer in the course of his or her privileged doctor / patient relationship with the prisoner.

- In cases where consent is obtained, care must be taken to limit the report to medical fact or opinion which is relevant for the purposes noted above. A comprehensive history would rarely be relevant for these reports.

12.4. An adjudication panel is entitled to request relevant information from a prison medical officer and in response the prison medical officer may properly provide such information. Medical reports to adjudication panels should only contain information relevant for the required purpose and not be excessive. Reports should be prepared on the basis of the medical officer's consultation with the prisoner at the time of the adjudication.

12.5. As with the disclosure of confidential information in any other circumstances, staff need to be aware of the potential consequences of a disclosure to the prisoner of any information or opinion which would be likely to cause any harm to the prisoner or any other person. In such cases, medical officers must make the panel aware of their concerns and have their views recorded.

12.6. At some point, it will be necessary for prison staff to share information with, and obtain information from, other agencies, for example, GPs, NHS providers, social care agencies. In all cases, the sharing of information between agencies should adhere to legal requirements such as the DPA 1998. If an individual wants information about them to be withheld from an agency, the individual's wishes should be respected unless there are exceptional circumstances that do not require consent.

Requests For Information

13. Requests from the media

13.1. Under no circumstances should personal or non-personal information be given out to the media. Staff who receive requests from the media in any format should forward and refer that person to the Trust Communication's Department by emailing

14. Requests from the police

14.1. The police do not have an automatic right of access to information held by CLCH. Where a request is received, certain information can be released without consent if there is a legal justification or requirement for disclosure.

14.2. Where the information is required to assist the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty, section 29 of the DPA can be applied. This section does not 'require' the disclosure of information; it merely provides CLCH with a legal basis under which it may release the information.

14.3. There is a legal duty that requires health professionals to release, where requested by police:

- The names of patients treated after a car accident to assist in the investigation of alleged dangerous driving.
- Medical records / information, human tissue or fluid, if the request is backed by a court order or search warrant.
- Medical records / information where there are reasonable grounds for believing the records are evidence in relation to an offence and it is necessary for police to seize them in order to prevent loss or alteration of evidence.

14.4. However, these requests must be made in writing using an official form. Under no circumstances should information be provided unless logged and authorised by the Caldicott Guardian or a member of the IG team.

15. Requests from solicitors

15.1. A request for personal information from a solicitor is still under the subject access provisions of DPA. A letter of authorisation or consent must accompany requests from solicitors for personal information of their client. Staff should make reference to the Access to Health and Personnel Records Code.

16. Public Interest

16.1. According to the 'Confidentiality: NHS Code of Practice' (2003), the public interest is: *'where exceptional circumstances justify overruling the right of an individual to confidentiality in order to serve a broader societal interest'*. Decisions about the public interest are complex and must take account of both the potential harm, that disclosure may cause and the interest of a free and democratic society in the continued maintenance of an individual's right to confidentiality. In all public interest decisions, staff should consult the Caldicott Guardian.

16.2. The public interest exemption can only be used if all the following conditions apply:

- Disclosure would be in the public interest; **AND**
- The purpose of the disclosure cannot be achieved with anonymised information; **AND**
- There is no statutory basis for disclosure (i.e. DPA) **AND**
- Patient consent has not been given because;

- **o** It is not practicable to ask the patient for consent e.g. because the patient contact details are out-of-date or the matter is urgent and the patient cannot be contacted, **OR**
- **o** It would be inappropriate to ask the patient for consent, e.g. they may lack the capacity to give consent or they are suspects who should not be informed they are under criminal investigation, **OR**
- **o** The patient has been asked for consent and has refused.

16.3. In order to share information on the basis of the 'public interest', it is important to gather relevant information such as:

- The purpose(s) served by the disclosure, and whether the purpose(s) could be served without the disclosure of confidential patient information.
- The individual(s) and/or organisation(s) affected by disclosure or non-disclosure, and the resulting level of detriment or benefit.
- The confidential information that is requested or required.
- The proposed recipient(s) of the disclosure, and whether they will disclose the information further.
- Whether there is either a statutory barrier or requirement to disclose
- Who should be involved in the decision and who will be accountable
- The urgency of the decision

16.4. Where confidential information is being disclosed for a purpose other than those as medical purposes in schedule 3 of the DPA then another justification must be found for the "processing", for example, *"functions of a public nature exercised in the public interest", "administration of justice*" and vital interests (matters of life and death).

16.5. The balance between serious harm to the individual to whom the information relates and serious harm to others must also be taken into account. Confidential information can be disclosed without consent to

prevent serious harm or death to others. This is likely to be defensible in common law in the public interest.

16.6. However, an individual's best interests are not sufficient to justify the disclosure of confidential information where he/she has the capacity to decide for him/herself. There has to be an additional public interest justification, which may or may not be in the patient's best interests.

16.7. Examples of where public interest can be a defence include:

- Reporting to the Driver & Vehicle Licensing Agency a patient who rejects medical advice not to drive (although health professionals should inform the patient of their intention to report it)
- Breaching the confidentiality of a patient who refuses to inform his or her sexual partner of a serious sexually transmittable infection
- Releasing relevant confidential information to social services where there is a risk of significant harm to a child.

17. Requests for personal information from staff and patients

17.1. Under the DPA, a person has the right to request access to their own record, otherwise known as a subject access request.

17.2. All requests must be made in writing and include identification of the data subject. By law, these must be responded to within 40 calendar days. Reference should be made to the *CLCH Access to Health and Personnel Records Policy*in such cases.

17.3. Employees may only access information relating to them by exercising their rights of access under the DPA, subject to the exemptions from access contained within the Act.

17.4. Staff who wish to access their HR record should contact the Head of Resourcing and Workforce information within the HR Department.

18. Requests for non-personal information

18.1. Requests for non-personal information are governed by the requirements of the Freedom of Information (FOI) Act 2000. Please refer to the *CLCH Freedom of Information (FOI) Policy* for details on how to handle FOI requests.

Patient/ service user engagement

19. Patient Choice

19.1. Patients have the right to choose as to whether or not personal information about them is disclosed. The disclosure of information for healthcare purposes is not normally an issue for the great majority of patients, however, where appropriate, patients must be given opportunities to raise objections and concerns. Patients also have the right to change their mind regarding the disclosure of their information.

19.2. As service users have the right to object to the use and disclosure of their personal information, it is important that they are made aware of this right. Sometimes, if a service user chooses to prohibit information being disclosed to other health professionals involved in providing care, it might mean that their care is limited and, in extremely rare circumstances, it is not possible to offer certain treatment options. Service users must be informed of their decisions regarding the disclosure of their information and the possible implications on their care or treatment. Health professionals cannot usually treat service users safely, nor provide continuity of care, without having relevant information about that service user such as their condition or medical history.

19.3. Advice about the use of patient information will be made available through the use of leaflets and posters displayed in appropriate areas. Contact information of the Caldicott Guardian and relevant staff will also be made

available to patients to provide a point of contact for patients to ask questions regarding the use of their information.

19.4. Patients also have the right to direct questions or concerns to other sources such as Patient Advice Liaison Service (PALS) or the Information Commissioner's Office.

20. Consent

See also CLCH Consent to Treatment and Examination Policy.

20.1. One of the main requirements for disclosing confidential information is to have the consent of the person in order to do so, in all cases this must be informed consent.

Informed Consent

20.2. Informed consent means the person giving consent understands

- Why information needs to be shared.
- Who may see their information.
- What it will be used for, and
- The implications of not sharing that information.

20.3. Evidently, patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. In order to inform patients properly, staff must:

I. Check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood.

II. Make clear to patients when information is recorded or health records are accessed.

III. Make clear to patients when they are or will be disclosing information with others.

IV. Check that patients are aware of the choices available to them in respect of how their information may be disclosed and used.

V. Check that patients have no concerns or queries about how their information is disclosed and used.

VI. Answer any queries personally or direct the patient to others who can answer their questions or other sources of information.

VII. Respect the rights of patients and facilitate them in exercising their right to have access to their health records.

Implied vs Explicit Consent

20.4. Consent can be established explicitly for example in written form, or may be implied for example, patient opening their mouth to let the doctor look at their throat.

20.5. Reliance on implied consent is particularly common in the healthcare sector. Implied consent is defined as ‘consent which is inferred from a persons’ conduct in the light of facts and matters which they are aware of, or ought reasonably to be aware of, including the option of saying ‘no’ (Department of Health Information Code, January 2001).

20.6. Consent does not need to be written, though a signed consent form, as evidence of consent, is good practice (explicit). Consent can also be expressed orally; in such cases staff should note this in the patient’s record.

20.7. However, where the disclosure of information involves personal sensitive information, consent must always be explicit in order to meet DPA conditions unless otherwise legally exempt.

21. When is Consent not required?

21.1. There are circumstances under which information can be shared without consent. For example:

- Where the subject does not have mental capacity and it is in their best interest to share information (an assessment of mental capacity would have to be conducted).
- To prevent or assist in the detection of crime.
- To protect the vital interest of the person concerned or another person, such as life and death situation or safeguarding purposes
- Disclosure is in the public interest.
- To comply with a court order.

22. Best Interests

22.1. According to the General Medical Council Confidentiality 2009, the health professional who is treating the individual should consider the following when deciding the best interests of the patient who lacks mental capacity to make choices regarding information sharing:

I. Make the care of the patient the first concern

II. Treat patients as individuals and respect their dignity

III. Support and encourage patients to be involved

IV. Treat patients with respect and not discriminate against them

22.2. The following should also be considered:

I. Whether the patient's lack of capacity is temporary or permanent

II. Which options for treatment would provide overall clinical benefit for the patient

III. Which option, including the option not to treat, would be least restrictive of the patients future choices

IV. Any evidence of the patient's previously expressed preferences, such as an advance statement or decision

V. The views of anyone the patient asks you to consult, or who has legal authority to make a decision on their behalf, or has been appointed to represent them

VI. The view of people close to the patient on the patient's preferences, feelings, beliefs and values, and whether they consider the proposed treatment to be in the patient's best interests

VII. What the healthcare team know about the patient's wishes, feelings, beliefs and values.

22.3. There are two circumstances where these principles will not apply. The first being, where someone has previously made an advance decision to refuse treatment whilst they had the capacity to do so. The second concerns the involvement of research, in certain circumstances.

Management of Risk

23. Information Governance Training

23.1. All staff employed by CLCH are required to complete online information governance training using the IG Training Tool. This can be accessed by clicking below or via the Connecting for Health website:

https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

23.2. Staff can register themselves on the system using the organisation code RYX. Staff who have access to personal data must complete ' An introduction to Information Governance' module and those who do not have access to personal data must complete ' The Beginners Guide' module.

23.3. Once these have been completed, the simple refresher module must be completed by all staff on an annual basis.

24. Incidents and Untoward Events

See also Risk Identification and Management Policy and Incident Reporting and Management Policy.

24.1. All events involving the loss of data, whether relating to service users, staff or the organisation must be reported. All information governance related incidents will be reported to the Information Governance Group for review and monitoring of frequency, severity and trends.

24.2. Any incident that could adversely affect the Organisation's reputation or impacts on greater than 20 people will be considered as serious and investigated using level 2 methodology. These events will be reported to the Strategic Health Authority and Information Commissioner. Serious incidents will be investigated with the support of the information governance team.

24.3. CLCH has a fair blame approach to managing untoward events. The involvement of staff will be considered in line with the NPSA's Incident Decision Tree (www.npsa.nhs.uk) and relevant CLCH human resources policies (available on the intranet).

25. Data Quality

See also CLCH Data Quality Policy

25.1. High quality information underpins the delivery of high quality healthcare and many other key service deliverables. Information has greatest value when it is accurate, up to date and accessible when and where it is needed.

25.2. It is a legal requirement to ensure the quality of data remains at a high standard. For example, the third principle of the DPA states the processing of personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Staff should seek the minimum amount of information that is required; it is not acceptable to hold information on the basis that it might possibly be useful

in the future without a view of how it will be used. The Trust will monitor compliance with this principle through record keeping audits across the Trust.

25.3. The fourth principle of the DPA states, *'Personal data shall be accurate, and where necessary, kept up-to-date'.* The Trust will make every effort to ensure that this is the case.

25.4. Data quality can also affect patient experience; if records are inaccurate or incomplete then future decisions may be wrong and potentially harm the service user. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors.

25.5. Overall, health records should be:

- Factual consistent and accurate.
- Written within a maximum of 24 hours of contact, providing current information on the care and condition of the patient.
- Written clearly, legibly and in such a manner that they cannot be erased.
- 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 clear.
- Clear, unambiguous and written in terms that the service user can understand.
- Relevant and useful.

25.6. Many difficulties with information sharing come about because the quality of information is inaccurate, or because an opinion is given as fact. Staff should make every effort to ensure data is reliable and consider the source from which the information originated.

25.7. Further guidance can be found in the Records Management Code, Clinical Records Keeping Standard and the Data Quality Code.

26. Retention and Storage of Records

See also CLCH Records Management Policy

26.1. Records containing personal and / or confidential information should not be kept for longer than necessary and stored appropriately. Guidance on retention periods and the storage of records is provided in the Trust's Records Management Code.

26.2. The duty of confidentiality continues from the creation of the information through to its ultimate destruction and disposal. CLCH operates a records retention schedule that should be referenced prior to the destruction of any information.

27. Consultation, Approval and Ratification Process

Identification of Stakeholders

27.1. This Policy was created following the formation of CLCH in line with guidance produced by the Information Commissioner's Office.

Consultation Process

27.2. Members of the CLCH Information Governance Committee, which includes clinical and non-clinical representatives, provided oversight into this Policy's development.

Equality Impact Assessment

27.3. CLCH aims to design and implement services, policies and measures that meet the diverse needs of its services, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Assessment Tool assesses the impact of this Policy and is attached.

Approval Process

27.4. This Policy has been developed by the Information Governance Team and approved by the Information Governance Committee.

27.5. This Policy has been ratified through the process outlined in the CLCH *Policy for the Development and Management of Procedural Documents* and has been ratified by the Executive Management Team.

Ratification Process

27.6. This Policy has been approved by the Information Governance Committee. It was reviewed by the Policy Advisory Group before receiving final ratification from the Executive Management.

Process for reviewing a Policy

27.7. This Policy will be reviewed in three years through full consultation with the Information Governance Committee, unless there are any changes in national guidance/ legislation or CLCH service provision which make earlier revision necessary.

Version Control

27.8. A final version of this document will be available on the CLCH intranet. It is the responsibility of the Information Governance Committee Chair to ensure that it is updated and available on the intranet.

Dissemination and Implementation

27.9. Notification of this Policy will be sent to all staff within the organisation.

27.10. CLCH has purchased Policy software which has been designed to notify specific members of staff when a Policy has been ratified (or minor changes to a current Policy have been made) of which they must be aware. The software will notify the staff member, track and monitor acceptance and, where appropriate, require the staff member to complete a test to ensure understanding before accepting the terms of the Policy.

27.11. It is the responsibility of all Senior Managers, clinical & operational leads to ensure implementation of this document. This Policy will be covered in Induction and Refresher Training sessions.

28. Audit Process

28.1. Regular monitoring reports will be received by the Information Governance Committee.

29. References

- Data Protection Act, Department of Health, 7th June 2011, gateway reference: 16108.http://www.dh.gov.uk/en/Managingyourorganisation/InformationCode/Recordsmanagement/DH_4000489
- Confidentiality: NHS Code of Practice – supplementary guidance; public interest disclosures, Department of Health, 22nd November 2010. http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/@ps/documents/digitalasset/dh_122031.pdf
- Confidentiality: NHS Code of Practice, Department of Health, 7th November 2003, http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4069254.pdf
- Information Commissioner Website, http://www.ico.gov.uk/for_organisations.aspx
- The Caldicott Manual 2010, Department of Health, Gateway reference 14043, 1st March 2010.
- Data Sharing Code of Practice, Information Commissioner's Office, May 2011.
- The Common Law Duty of Confidentiality, Department of Health, Available at http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsCodeAndGuidance/Browsable/DH_5803173
- Gillick v Norfolk and Wisbech Area Health Authority, House of Lords, 17th October 1985. Available at http://www.hrcr.org/safrica/childrens_rights/Gillick_WestNorfolk.htm
- Consent: A guide for children and young people, Department of Health, 16th July 2001, Available at

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsCodeAndGuidance/DH_4008977

- The Data Protection (Subject Access Modification) Order 2000, 17th February 2000, no. 413. Available at http://www.legislation.gov.uk/uksi/2000/413/pdfs/uksi_20000413_en.pdf

- NHS Choices, Consent to Treatment, Available at: http://www.nhs.uk/Conditions/Consent-to-treatment/Pages/How-does-it-work.aspx

- General Medical Council Confidentiality 2009; Confidentiality guidance: Disclosures about patients who lack capacity to consent. Available at: http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_57_63_patients_who_lack_capacity.asp

- Guidance on the protection and use of confidential health information in prisons and inter-agency information sharing; information and practice 2002:

  https://nww.igt.connectingforhealth.nhs.uk/KnowledgeBaseNew/DH_Protection%20and%20Use%20of%20Confidential%20Information%20in%20Prisons.pdf

Appendix A: Declaration Form

Form for all employees to sign – including contracted employees, non-contract employees such as: bank, agency, volunteers, locums, student placements, suppliers.

During the course of your time working for, or on behalf of, Central London Community Healthcare ('CLCH'), you may acquire or have access to personal and / or confidential information. All employees (including those listed above) have a duty of confidence towards patients and staff and must not disclose such information to any person unless this is in pursuit of your duties or with specific permission given by the person concerned or the Caldicott Guardian / IG Team. This duty of confidence applies at all times, both during and after your time working for CLCH.

All information relating to service users and business information concerning the Trust or its affairs should be treated as confidential. If you are in doubt as to what information may be disclosed, you should check with your manager.

The DPA regulates the use of personal information in both electronic and paper format. The Trust is registered in accordance with this legislation and any breach of this legislation may lead to legal or disciplinary proceedings.

I understand that I am bound by a duty of confidentiality. I have read, understood and agree to adhere to the Code of Conduct and the legal, national requirements it highlights such as the DPA.

PRINT NAME:	
SIGNATURE:	
DATE:	
ON BEHALF OF THE TRUST It is clear that the staff member has read and understood the Code of Conduct.	
WITNESS / MANAGER'S NAME:	
SIGNATURE:	
DATE:	

Appendix B: Staff Confidentiality Code of Conduct; key points to remember!

1. **Have Confidence!** – a duty of confidence is the expectation that information disclosed will be held in confidence and is a legal, contractual and professional requirement.
2. **Obey the Law** – see section 6 for the main legal and contractual requirements to consider when it comes to the use of personal information, e.g. the DPA.
3. **Caldicott –** the six Caldicott principles must be applied at all times when handling personal and confidential information so only use it when absolutely necessary….and so on!
4. **Do not share** – remember that you will be held responsible for any activity carried out in your name so it is important that you do not share things like your password, security pass, smartcard.
5. **Use information properly** - only access confidential information for work purposes, don't look at information about friends, relatives, celebrities or even yourself.
6. **Treat others as you wish to be treated** – or, treat other people's information the way you would like them to treat yours! Collect computer printout and faxes as soon as possible, be careful not to leave originals inside the photocopier or fax, don't leave paper lying around, file them or destroy them when you are finished. Dispose of data appropriately using the confidential bins and not just any bin.
7. **Be aware** - make sure someone isn't eavesdropping when discussing confidential information, particularly in a public place or over the telephone.
8. **Take responsibility** - don't assume someone else will pick up a loose file, if you see a potential data security breach, take appropriate action to protect the data and report the incident.
9. **Use computers properly** - use IT equipment, email and internet facilities properly. Be sensible, if it feels wrong then it probably is wrong, read the guidance and policies of the Trust and abide by them.
10. **Get Help** - if in doubt contact your manager or the IG Team for advice. You should be trained to use the information properly in your job but this does not replace your common law duty of care, if you need more training you should ask.

Equality Impact Assessment

1. Protected characteristic Does the policy affect groups of people based upon their protected characteristic?	**Specify if the impact is positive, negative or neutral and why. See guidance.**	**Response – State if further review is required, time period and ways to minimise any negative impact.**
People of different ages (eg. Children, young or older people).	Positive	Details of consultation with staffs are contained within section 25 of the policy. Implementation of this policy will protect the human rights of staff, patients, visitors and the public to confidentiality. It also guides access to information held about them. This policy will be made available on the intranet and extranet. It is available in English but can be translated upon request. The organisation will monitor the application of this Policy, on at least an annual basis, and will consider the action needed to maximize any adverse impacts.
People of different religions / beliefs	Positive	
People with disabilities (physical, sensory or learning).	Positive	
People from different ethnic groups	Positive	
Men or women	Positive	
Transgendered people	Positive	
People who are gay, lesbian, and bi-sexual	Positive	
Refugees and asylum seekers	Positive	

2	Is more information or analysis needed before making a reasonable assessment about the negative impact of the policy?	Yes Go to section 3	**No (+)** Go to section 4
3	If 'yes' to section 2, can the proposal be delayed to allow time to collect the necessary information?	Yes contact the Head of Equality Diversity and Human Rights	No Go to section 6

4	Does the policy need a full Equality Impact Assessment to be undertaken?	Yes contact the Head of Equality Diversity and Human Rights	**No** Go to section 5	
5	Please describe the evidence used in reaching the assessment in section 1. (e.g. Organisation data, results of consultation, community views, external data, and external reports). ***Details of consultation with staffs are contained within section 25 of the policy. Implementation of this policy will protect the human rights of staff, patients, visitors and the public to confidentiality. It also guides access to information held about them.*** ***This policy will be made available on the intranet and extranet. It is available in English but can be translated upon request.***			
6	**Please describe the rationale for proceeding with the policy in its current form**. You should include this information in the report to the executive management committee or CLCH Board (*?), as appropriate.			
7	If negative impact *is* indicated in section 1, are there any changes which can be made to the proposal now which could reduce or remove the risk of this negative impact?	Yes Incorporate changes prior to finalising. Go to section 8.	**No** Go to section 8	**Not applicable (+)** i.e. no negative impact indicated **go to section 8**
8 a b c	Conclusion: Following initial screening the policy will *(bold as appropriate)*: **the proposal will be submitted without amendment (+)** the proposal will be submitted in amended form the full equality impact assessment will be undertaken before submitting the proposal for decision			

Signed for team / working group: Name …… Date ……

Training Needs Analysis

	Response
There is no specific training requirements - awareness for relevant staff required, disseminated via appropriate channels. (Do not continue to complete this form-no formal training needs analysis required.)	☐
There is specific training requirements for staff groups	☑

Staff Group	Y/N	Frequency	Suggested Delivery Method
Clinical patient contact:	☑	**Annual**	Face to face Team based sessions Induction and mandatory refresher sessions Online learning via connecting for health
Registered Nurse	☑	**Annual**	
Care Assistant	☑	**Annual**	
Health Visitor	☑	**Annual**	
Therapist	☑	**Annual**	
Clinical bank staff worker	☑	**Annual**	
Non-clinical patient contact	☑	**Annual**	
Non-clinical non-patient contact	☑	**Annual**	

Please give the source that has informed the training requirement outlined within the policy, i.e. National Confidential Inquiry/NICE guidance etc.

Health & Social Care Act, Caldicott, Data Protection Act, Freedom of Information Act

Signed for team / working group: Name …… Date ……

Dissemination Record - to be used once document is approved.

Date put on register of procedural documents		Date due to be reviewed	

Disseminated to: (either directly or via meetings, etc)	Format (i.e. paper or electronic)	Date Disseminated	No of Copies Sent	Contact Details / Comments

Training Record - once document is approved.

Date sent to Learning & Development / Training & Education team:	

Document Control Sheet

Document purpose
This document sets forth CLCH's expectations of staff in relation to managing information.

Key words
Best interests, Caldicott Principles 1998, Children and young people, Common Law Duty of Confidentiality, Computer Misuse Act 1990, Crime and Disorder Act 1998, Data Protection Act (DPA) 1998, Data quality, Data sharing, Explicit consent, Freedom of Information (FOI) Act 2000, Human Rights Act 1998, Implied consent, Information Commissioner's Office, Information sharing, Informed consent, Media, Non-personal information, Patient choice, Patient information, Personal data, Personal information from staff and patients, person-identifiable data, Police, Public interest, Retention, Sensitive personal data, Solicitors, Staff information, Storage.

Target audience
This policy applies to all staff working for, or on behalf of, CLCH and includes those staff on honorary contracts, contractors/ agency workers and students.

Effective from:	**Effective to:**	**Review in:**
October 2011	October 2014	June 2014

Version	**Date**	**Summary of change**
1	30.09.11	First CLCH version. Created post formation of CLCH using legacy organisation procedural documents. **Ratified by PAG on 19.10.11**

Stakeholder Reviews *This document has been reviewed for factual accuracy by the following before being submitted for final approval*	
Name/ Group	**Date**
Information Governance Group	30.09.11

Approval and Ratification *This document has received the following approvals*	
Title/ Committee	Date
Policy Advisory Group	19.10.11

Paper information *Please forward all correspondence and comments to:*	
Name/ Group	Role
S Dawson (Information Governance Facilitator) S Wilkins (Head of Information Governance & Management)	Author
K Stone (Director: Clinical Leadership, Governance, Quality and IM&T)	Owner

Related guidance
Please consider this document in conjunction with the following documents

- Risk Identification & Management Policy
- Incident Reporting & Management Policy
- Freedom of Information Policy
- Subject Access Request Policy
- Records Management Policy
- Transfer of personal information Policy