Information Sharing Policy and Data Protection Act

Author	Not Available
Responsible Director	Managing Director
Ratified By	Quality and Safety Committee
Ratified Date	
Review Date	December 2015
Version	1.0
Policy Consultation Period	21.01.2015 – 20.02.2015

Related Policies & Guidelines:

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

Contents

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.0		December 2014	Initial policy for consultation	

1. Policy Summary

The purpose of this 'Data Protection Act and Information Sharing Policy' is to build on the guidance contained within the Information Governance overarching policy and provide specific guidance relating to compliance with the Data Protection Act 1998 and to Information Sharing in particular.

It links to Central London Healthcare's overarching Information Governance Policy which sets out the minimum policy standards for confidentiality, integrity and available of information. It covers the overlapping areas of data protection compliance (including Caldicott), information security (ISO27002 – Code of Practice for Information Security), data quality, confidentiality (with regard to 'common law'), records management and compliance with legislative requirements such as Data Protection Act 1998, Freedom of Information Act 2000 and other related legislation that is relevant to information handling.

Central London Healthcare (CLH) has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty to comply with guidance issued by the Department of Health, the NHS England, other advisory groups to the NHS and guidance issued by professional bodies.

2. Roles and Responsibilities

2.1 Head of Performance and Information / Information Governance Manager

The Head of Performance and Information also carries the role of Data Protection Officer for CLH as a Data Controller (sometimes also known as the privacy officer). As such they are the designated contact with the Information Commissioner on behalf of CLH for all data protection issues. The main features of this role will be to provide advice and support to CLH whilst leading on audit and improvement plans relating to information governance. The Data Protection Officer is responsible for maintaining CLH's data protection notification with the information Commissioner and ensuring the Trust's on-going compliance with the Data Protection Act 1998, including advising the Caldicott Guardian on points of interpretation, particularly where issues arise as a result of the interface between the Act and the use of technology.

2.2 Caldicott Guardian

The Caldicott Guardian is the executive with Board level responsibility to ensure CLH complies with the Data Protection Act 1998. This role gives both support to the Information Governance Manager with a direct channel to progress issues, and emphasises to all staff the importance of implementing and ensuring compliance with statute.

The Caldicott Guardian is responsible for compliance with the Caldicott principles. The role is responsible for establishing and maintaining procedures governing access to, and the use of, patient identifiable data held or processed within systems or networks which are the responsibility of CLH. The Guardian will also agree local procedures and protocols to ensure consistency with any relevant central requirements and guidance.

2.3 Senior Information Risk Officer (SIRO)

The Senior Information Risk Officer (SIRO) is the Manager who is responsible for taking ownership of CLH's information risk policy. This role is allocated to the Head of Performance and Information. This includes acting as an advocate for information risk on the Board and providing written advice to the accounting officer on the content of their Statement of Internal Control in regards to information risk.

3. Definition of Terms

3.1 Personal data

Personal Data means information which relates to a living individual who can be identified:

- From those data, or
- From those data and other information which is in the possession of , or is likely to come into the possession, of the data controller

3.2 Sensitive personal data

Sensitive Personal Data means personal data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- His religious beliefs or other beliefs of a similar nature
- Whether they are member of a trade union
- Their physical or mental health conditions
- Their sexual life
- The commission or alleged commission by him of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by the person

4. Principles of the Data Protection Act

CLH is committed to upholding the eight principles of good practice contained within the 1998 Data Protection Act. These relate to both digitally and manually held data. The following sets out how all staff in CLH should comply with the principles of the DPA.

4.1 First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- CLH will provide and promote materials for patients and staff that identify how their information is processed and protected. This will form the basis of 'informed consent' for general uses of information. This will to a reasonable extent meet the condition of consent for processing of personal data. Consent is defined as "any

freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

- For the processing of sensitive data (including physical or mental health or condition), most activity will be compliant under schedule three, condition eight – 'processing is necessary for medical purposes and is undertaken by a health professional of person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. ('Medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health services').
- CLH will actively develop, in line with national policy direction, systems to record the wishes of patients that are expressed in response to information presented to them.
- CLH will maintain an accurate, up to date data protection notification with the Information Commissioner on the purposes, sources, subjects and disclosures of data it uses. The Trust's notification will detail the specified and lawful purposes that data shall be obtained and processed for.
- CLH will pseudonymise data being used for secondary purposes where it is reasonably practicable to do so.

4.2 Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- CLH's data protection notification to the Information Commissioner will detail the specified and lawful purposes that data shall be obtained and processed for.
- CLH will actively participate in protocols for information sharing between organisations to ensure that further processing and sharing is carried out in a manner compatible with the principles. The purposes should be compatible with the notification. This is provided the protocols are set out within the boundaries of applicable legislation and regulation and do not compromise the organisation or the confidentiality of the personal/sensitive data that it holds.

4.3 Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- CLH will conduct routine audits/reviews as part of good data management practice to ensure that information collection is adequate, relevant and not excessive.

4.4 Fourth Principle

Personal data shall be accurate and, where necessary, kept up-to-date.

- CLH will ensure that personal information held on any media is accurate and up to date. Validation processes and routines will be developed, utilised and maintained.

- Users of software will be responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.
- Staff will check with patients that the information held by CLH is kept up to date by asking patients to validate the information held.
- Information held on staff will also be checked for accuracy on a regular basis – either by the manager or by the Human Resources/Personnel department.
- CLH in signing up to Information Sharing agreements or specific subject policies (such as vulnerable adults) will ensure that the accuracy of data shared between organisations is covered in the agreement.

4.5 Fifth Principle

Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose or those purposes.

- CLH will instigate retention and disposal procedures of all identifiable (and other records held) in line with central NHS guidance – currently Records Management: NHS Code of Practice, published by the Department of Health in March 2006.

4.6 Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

- CLH will ensure that a formal process for patients/staff to request access to their records is in place and that a response will be achieved within required timescales.
- Handling subject access requests made by, or on behalf of, a current or past patient will be dealt with by CLH's Quality and Project Coordinator. In some circumstances advice from the Trust's Caldicott Guardian and/or Data Protection Officer may also be sought. The Freedom of Information Act provides access to all types of recorded information (not personal information) held by the Trust. Reference should be made to the Information Governance: Freedom of Information Act 2000 policy for these requests.
- Any member of staff current, past or potential (applicant) who wishes to have a copy of their information under the subject access provision of the Data Protection Act will need to contact, in writing, Human Resources at CLH.
- The Act requires that requests are responded to within 40 calendar days. CLH will log all requests received and will reply promptly, following payment of any necessary fee. (This time is calculated from the day on which the Trust has received the required fee and any necessary information to confirm the identity of the individual making the request). There are certain circumstances where information can be withheld from a subject access request. Access can be denied or limited where the information might cause serious harm to the physical or mental health or condition of the patient or any other person or where giving access would disclose information relating to or provided by a third person who has not consented to disclosure.

- Information will be provided in a permanent form unless this causes CLH 'disproportionate effort' or the patient agrees to receive it in another form. The data supplied must be intelligible and any lengthy abbreviations explained.
- Factual information in patient records that is inaccurate will be corrected. However if the patient disputes the accuracy, but the clinician maintains the information is correct, the information will remain unchanged. However, the patient's view will be added to the notes to indicate there is discrepancy between the recorded information and the patient's viewpoint.
- The Access to Health Records Act 1990, and not the DPA 1998, provides guidance on the access rights of relatives, or those who may have a claim, to deceased patients records.

4.7 Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Obtaining, holding, use, or disclosure of information

  All information relating to identifiable individuals must be kept secure at all times, whether personal data is held in paper format or electronic format. All staff will ensure there are adequate and reasonable procedures taken to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Areas containing patient identifiable information must either be supervised, to prevent unauthorised access, or be secure so that no entry can be gained by unauthorised individuals. Identifiable information on patients and staff will only be disclosed on a strict need to know basis. Some disclosures of information may occur because there is a statutory requirement upon CLH to disclose e.g. with a Court Order, or because other legislation requires disclosure (tax office, pension agency - for staff and notifiable diseases - for patients). Further guidance is provided within the NHS Confidentiality Code of Practice and advice can be obtained from the organisation's Information Governance Manager.

- Destruction of personal identifiable information

  CLH has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and CLH business. It is important that this information is disposed of in a secure manner when no longer required. Health records will be maintained and disposed of in accordance with the NHS Records Management Code of Practice and a record kept of all records destroyed. The Trust will provide a secure confidential waste disposal facility for every department processing personal identifiable information.

- IT System Security

  The organisation is responsible for ensuring that all its IT systems and its users comply with current data protection and associated legislation i.e. Computer Misuse Act. This will include responsibility for ensuring that the registration of the system is

kept up to date and that procedures are in place to achieve a high level of data quality. Further guidelines are provided in the Information Governance Policy and the Information Security Policy.

- Transportation and Transfer of Personal Identifiable Information
  Detailed guidance is provided to staff on how to securely communicate personal identifiable data whether by phone, royal mail post or courier, email or fax. This is contained in the Safe Haven Policy and Confidentiality Policy.

- Security of Third Party Access
  Contractual arrangements will exist with third parties, suppliers, volunteers and other individuals/organisations. This will include an agreement outlining the need for confidentiality control and how this will be applied when the responsibility for information processing has been outsourced to another organisation, arrangements must address the risks and required security controls in the contract between the parties.

- Electronic Office Systems
  For electronic office systems such as calendar systems (such as Outlook), word processing, spreadsheets, databases, the following policy standards will apply:
    - An individual user is responsible (along with their line manager) for controlling access to their calendar and similar functions.
    - Users of database tools are required to adhere to the authorisation for new information processing control.
    - CLH will provide an infrastructure allowing staff to save files to shared network drives that are regularly backed up.
    - Departmental/line managers are responsible for defining who is allowed access to appropriate shared network drives.
    - Users are responsible for deleting files when no longer required and will regularly purge their folders.

- Electronic Mail
  An acceptable use policy exists that seeks to reduce risk from misuse, viruses and system failure. This details the criteria by which email will be monitored and that consent will be obtained for investigations unless it would prejudice such activity. The following provides a summary of permitted/non permitted use:
    - Permitted use of email for business purposes, includes sending patient data via NHS Mail or nhs.net only. The email must be from an nhs.net account to an nhs.net account so that the content is encrypted and secure. The only exception to this would be if it was in the vital interests of the patient, i.e. in a situation where their life was at risk. Limited personal use is also permitted.
    - Non permitted use includes excessive personal use or use for private gain, sending offensive, defamatory material or breaching confidentiality via

email, misrepresenting CLH or entering into contractual agreements and using email accounts other than your own or generic email accounts.

- Publicly Available Systems
  Access for staff to publish information to Trust websites will be controlled by a request and authorisation process. Content will be routinely monitored and removed when out of date.

- Information Exchange (phone, fax and post)
  No personal information shall be given out over the phone without the best endeavours by staff to confirm the identity of the other party and the wishes of the individual concerned. Phone calls that may feature personal or sensitive information shall be made in private areas if possible. Answer phone messages will only be left in 'urgent' situations and only minimal information will be provided.

  Detailed guidance regarding this and regarding fax usage is contained within the Safe Haven Policy.

  All mail should be correctly addressed, collected and delivered. If the correspondence is confidential, it should be sent to named individuals where possible.

  Processes will be in place to ensure that correspondence is sent to the correct GP or patient.

  Equipment, information or software will not be taken off site without appropriate authorisation. Equipment will be subject to a process of logging in and logging out. Formal records e.g. health records will be subject to a tracking system that incorporates this.

- Prevention of Theft of Information and Information Processing Facilities
  Where possible, paper and computer removable media, such as CD's, DVD's and back-up tapes, should be stored in suitable lockable cabinets when not in use. Patient information should be locked away when not required. Computers should not be left logged on when unattended. Information must not be left unattended on printers or fax machines.

4.8 Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection for the Rights and freedoms of data subjects in relation to the processing of personal data.

- Anyone needing to transfer data outside the EEA should take advice from the organisation's Data Protection Officer prior to doing so. There are conditions where the eighth principle does not apply, but these have to be considered individually.

5. Data Sharing

In May 2011 the Information Commissioner's office (ICO), published its Code of Practice on Data Sharing. It is a statutory code and should therefore be followed both in spirit and in practice. The code covers the two main types of data sharing:

- Systematic, routine data sharing between organisations
- Exceptional, one-off decisions to share data for any range of purpose

5.1 Sharing with a 'data processor'

This is the form of data sharing where CLH decides to share its data with another party that will process the personal data on our behalf.

The DPA requires that a data controller using a data processor must ensure there is a written contract in place. CLH policy requires exactly this to be followed when suppliers or contractors are engaged to conduct work for CLH, and where personal information will be shared with that supplier.

Before sharing any personal data, whether belonging to staff or patients, staff need to consider all the legal implications of doing so.

Regular, routine exchanges of information using confirmed secure methods of sending the data will not present so many problems as new, one-off requests, which may need to be carefully reviewed.

Advice must be sought from the Information Governance Manager, to ensure there are no legal constraints on the proposed sharing.

5.2 Factors to consider

- What information should be shared?
  The minimum amount of information should be shared with these who either need to know or have a statutory right to the information. It is often easier to send a whole report or spreadsheet then to extrapolate required fields only.

- How should it be shared?
  Staff should consider the most secure way to send the data. Detailed advice is available in the from CLH's Information Governance Manager.

- Could the Information be anonymised?

It is not appropriate to use personal data to plan the provision of services, for example, where this could be done with information that can be anonymised and would therefore not amount to personal data.

5.3 Information sharing agreements (ISA's)

The ICO Code of Practice Code on Data Sharing states when personal data is shared, it is good practice for the organisation disclosing it to make sure that it will continue to be protected with adequate security by any other organisations that will have access to it. The organisation disclosing the information should ensure that the receiving organisation understands the nature and sensitivity of the information. It is good practice to take reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement. Please note, though, that the organisations the data is disclosed to will take on their own legal responsibilities in respect to the data, including its security.

There should be clear instructions about the security steps which need to be followed when sharing information by a variety of methods, for example phone, fax, email or face to face.

CLH's Information Governance Manager will provide expert advice on the suitability of ISA's and provide the templates to be used.

6. Education and Training

Information Governance Training is an annual mandatory requirement and includes the following:

- confidentiality of personal information
- awareness of relevant policies and procedures
- compliance with Data Protection Principles
- individuals rights
- general good practice guidelines covering security and confidentiality
- an awareness of who to contact for all problems which may occur in the areas of security and confidentiality of personal information
- interaction with other required legislation i.e. Freedom of Information Act 2000.

To reduce the risks of human error, theft, fraud or misuse of facilities, responsibilities for data protection will be addressed during recruitment and will be included in employee contracts. All CLH employees will be made aware of their responsibilities through their Terms and Conditions of Employment.

All user training on systems will include education on appropriate policy and procedure elements for that system. These will focus on both security and data quality elements. Procedure guidance will be made available to staff to enable correct use of either CLH or departmental IT systems.

Training (via e-learning) in data protection and related legislation and codes of practice will be made available for staff.

The organisation (in conjunction with other providers/organisations) will provide ad-hoc training on an as-needs basis.

Appendix 1 – References

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

Information Security Management: NHS Code of Practice
http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf

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

Records Management: NHS Code of Practice
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

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

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

Information Commissioner's Office, Data Sharing code of practice
https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/