Confidentiality Policy

Author	Aleksandra Foy, Office Manager
Responsible Director	Medical Director
Ratified By	Quality and Safety Committee
Ratified Date	May 2014
Review Date	December 2015
Version	1

Related Policies & Guidelines:

- Information Governance Policy
- Safe Haven Policy
- Disciplinary Policy
- Confidentiality Code of Conduct
- Information Sharing Policy

Contents

Amendment History

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

1. Policy Summary

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within Central London Healthcare CIC (CLH) and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 1998. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

It is important that CLH protects and safeguards person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non NHS organisations.

1.1 Person-identifiable information

Person-identifiable information is anything that contains the means to identify a person, e.g.

- Name
- Address
- Postcode
- date of birth
- NHS number

This information must not be stored on removable media unless it is encrypted as per current NHS Encryption Guidance or a business case has been approved by the Information Governance Committee.

1.2 Confidential Information

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes CLH confidential business information.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

A summary of Confidentiality Do's and Don'ts can be found at Appendix 1.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles

of this policy can be found in Appendix 2.

How to report a breach of this policy and what should be reported can be found in Appendix 3.

Definitions of confidential information can be found in Appendix 4.

2. Scope

Staff of the following CLH areas are within the scope of this document:

- Staff working in or on behalf of CLH (this includes contractors, temporary staff, seconded staff, Executive Board Members and all permanent employees).
- Patient Panel Members

3. Roles and Responsibilities

3.1 The Managing Director

The Managing Director has overall responsibility for strategic and operational management, including ensuring that CLH policies comply with all legal, statutory and good practice guidance requirements.

3.2 The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

3.3 The Quality and Safety sub-committee

An Quality and Safety sub-committee will be established to oversee the development and implementation of Information Governance and ensure that the organisation complies with supporting the Legal and NHS Mandatory Framework with regard to Information Governance.

3.4 Manager with responsibility for HR

The Manager with responsibility for HR (currently Tom James, Service Delivery Manager for PRS and PCP) is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that the Confidentiality Policy is included in corporate inductions for all staff.

3.5 Senior Managers

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Procedure.

3.6 Information Governance Lead (Head of Performance and Information)

The Information Governance Lead is responsible for maintaining the currency of this policy, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

3.7 All Staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness-raising sessions carried out to inform and update staff on confidentiality issues.

Any breach of confidentiality, inappropriate use of health or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported.

4. Corporate Level Procedures

4.1 Principles

All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
- Access to person-identifiable or confidential information must be on a need-to-know basis
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information, that decision must be justified and documented
- Any concerns about disclosure must be discussed with your Line Manager or Information Governance Lead/Head of Performance and Information.

CLH is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Access to rooms and offices where terminals are present or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by key fobs. In mixed office environments, measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular, they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

4.2 Disclosing Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager or Information Governance Lead before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority.
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager or Information Governance Lead before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

If staff members have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance Lead/Head of Performance and Information.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the Information Governance Committee or see the Information Sharing Policy.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. See the Safe Haven Policy for guidance on the safe transfer of confidential or person-identifiable information.

Transferring patient information by email to anyone outside the CLH network may only be undertaken by using encryption as per the current NHS Encryption Guidance or through an exchange within the NHS Mail system (i.e. from one NHS.net account to another NHS.net account or to a secure government domain e.g. gsi.gov.uk), since this ensures that mandatory government standards on encryption are met. Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

4.3 Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry CLH information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents. Taking home/removing paper documents that contain person-identifiable or confidential information from CLH premises is discouraged and, if required to do so, staff should use encrypted data sticks.

When working away from CLH locations staff must ensure that their working practice complies with CLH's policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

Staff must minimise the amount of person-identifiable information that is taken away from CLH premises.

If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of CLH buildings
- Confidential information is kept out of sight whilst being transported

- Employees should consider, understand and acknowledge all risks involved in transfer of the information and accept personal liability for breaches of the Data Protection Act 1998 and Contract of Employment

If staff do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately owned computer or device.

4.4 Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard
- Leave any person-identifiable or confidential information lying around unattended; this includes telephone messages, computer printouts, faxes and other documents
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended

Steps must be taken to ensure physical safety and security of person- identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

4.5 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of CLH.

If staff have concerns about this issue they should discuss it with their Line Manager or Information Governance Lead/Head of Performance and Information.

4.6 Confidentiality Audits

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the IG Lead with support from Information Governance Committee through a programme of audits.

5. Distribution and Implementation

5.1 Distribution Plan

This document will be made available to all Staff upon Induction and accessible for further reference via the CLH shared folders.

A global notice will be sent to all Staff notifying them of the release of this document.

5.2 Training Plan

A training needs analysis will be undertaken with Staff affected by this document.

Based on the findings of that analysis appropriate training will be provided to Staff as necessary.

6. Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Committee, together with independent reviews by both Internal and External Audit on a periodic basis.

The Information Governance Lead is responsible for the monitoring, revision and updating of this document.

7. Equality Impact Assessment

This document forms part of CLH's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this document and its impact on equality has been analysed and no detriment identified.

Appendix 1: Confidentiality Do's and Don't's

Do's

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation for everyone working on or behalf of CLH.

- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.

- Do ensure that you cannot be overheard when discussing confidential matters.

- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.

- Do share only the minimum information necessary.

- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.

- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.

- Do report any actual or suspected breaches of confidentiality.

- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.

- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.

- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.

- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix 2: Summary of Legal and NHS Mandated Frameworks

CLH is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of CLH, who may be held personally accountable for any breaches of information security for which they may be held responsible. CLH shall comply with the following legislation and guidance as appropriate:

The Data Protection Act (1998) regulates the use of "personal data" and sets out eight principles to ensure that personal data is:

1. Processed fairly and lawfully.
2. Processed for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date.
5. Not kept longer than necessary, for the purpose(s) it is used.
6. Processed in accordance with the rights of the data subject under the Act.
7. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data
8. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

The Caldicott Report (1997) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law.

Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1) Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2) Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3) Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.
    a) Making, supplying or obtaining articles for use in offences 1-3

The NHS Confidentiality Code of Practice (2003) outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made.

Our 12 commitments to you (Patients)

1. When we receive a request from you in writing, we must normally give you access to everything we have recorded about you. We may not give you confidential information about other people, or information that a healthcare professional considers likely to cause serious harm to the physical or mental health of you or someone else. This applies to paper and electronic records. However, if you ask us to, we will let other people see health records about you.

   Wherever possible, we will make your health records available to you free of charge or at a minimum charge, as allowed by law. We will provide other ways for you to apply to see your records if you cannot do so in writing.

   We will provide information in a format that is accessible to you (for example, in large type if you are partially sighted).

2. When we provide healthcare, we will share your record with the people providing care or checking the quality of care (unless you have asked that we limit how we share your record). Everyone looking at your record, whether on paper or computer, must keep the information confidential.

   We will aim to share only as much information as people need to know to play their part in your healthcare.

3. We will not share health information that identifies you (particularly with other government agencies) for any reason other than providing your care, unless:
    - you ask us to do so;
    - we ask and you give us specific permission;
    - we have to do this by law;
    - we have special permission for health or research purposes; or
    - we have special permission because the public good is thought to be of greater importance than your confidentiality

    If we share information without your permission, we will make sure that we keep to the Data Protection Act 1998, the NHS confidentiality code of practice and other national guidelines on best practice. There is more information about existing guidelines at: http://www.dh.gov.uk/

4. Legally, no-one else can make decisions on your behalf about sharing health information that identifies you. The only exceptions to this are parents or legal guardians, or people with legal powers to make decisions on behalf of adults who cannot make the decision for themselves or who may be a risk to others. You can appoint someone to have a lasting power of attorney to make decisions for you if you are losing the ability to make decisions for yourself. You can decide what rights that person has in making decisions about your care record. If you do not appoint anyone, a senior healthcare professional involved in your care may consider it to be in your best interests to share information. This judgment should take account of the views of your relatives and carers, and any views you have already recorded. For medical research or other purposes (see the details listed below), the National Information Governance Board for Health and Social Care advises when special permission should be given to share any health information that could identify individuals.

    When we might use or share information that names you without asking you

    Sometimes we have a legal duty to give information about people. Examples include:
    - registering births;
    - reporting some infectious diseases;
    - reporting gunshot wounds to the police; or
    - because a court orders us to do so.

    Sometimes special permission will be given to use information that identifies you without your consent. This may be for medical research, keeping registers of cancer patients or checking quality of care. This permission is given by the Secretary of State for Health on advice from the National Information Governance Board for Health and Social Care under strict conditions.

    Special permission may also be given when the public good outweighs your rights to confidentiality. This is very rare, but some situations where this might happen include:
    - when a serious crime has been committed;
    - when there are serious risks to the public or NHS staff; or
    - to protect children or vulnerable adults who are not able to decide for themselves whether their information should be shared.

Other than in the most exceptional circumstances, this permission is given by the senior clinician in charge of protecting your privacy in each health or care organisation. (Often this person will be called the Caldicott Guardian.)

5. Sometimes your healthcare will be provided by members of a care team, which might include people from other organisations such as social services or education. We will tell you if this is the case. When it could be best for your care for your health information to be shared with organisations outside the NHS, we will agree this with you beforehand. If you don't agree, we will discuss with you the possible effect this may have on your care and alternatives available to you.

6. Usually you can choose to limit how we share the information in your care records which identifies you. In helping you decide, we will discuss with you how this may affect our ability to provide you with care or treatment, and any alternatives available to you.

7. We will deal fairly and efficiently with your questions, concerns and complaints about how we use information about you. All trusts have a Patient Advice and Liaison Service (PALS) which can answer questions, point people towards sources of advice and support, and advise on how to make a complaint. We will have a clear complaints procedure. We will use what we learn from your concerns and complaints to improve services.

8. We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We will normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you feel you are suffering distress or harm as a result of information currently held in your record, you can apply to have the information amended or deleted.

9. We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and, how it applies to all parts of their work.

   All organisations providing care for the NHS or on our behalf must follow the same strict policies and controls. This is managed through the Department of Health's Information Governance Framework for Health and Social Care, and through the individual standards which make up the Information Governance Toolkit.

10. We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them. There may be times when someone will need to look at information about you without you giving your permission first. This may be justified, for example, if you need emergency care.

11. We will keep a record in the newer electronic record systems of anyone who has accessed a health record or added notes to it. Some of the older computer systems will only record who

has accessed a record where they have made changes. Paper records only include where people have made notes in the record and not when someone looks at the record.

12. If you believe your information is being viewed inappropriately we will investigate and report our findings to you.

    If we find that someone has deliberately accessed records about you without permission or good reason, we will tell you and take action. This can include disciplinary action, which could include ending a contract, firing an employee or bringing criminal charges.

Appendix 3: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to the Line Manager who is responsible for updating incident / Caldicott Issue Log and informing the Information Governance Lead and/or Information Governance Committee. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or Information Governance staff.

The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to CLH systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person-identifiable information in ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or Information Governance staff should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the Information Governance Committee.

The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix 4: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information as defined by the Data Protection Act 1998 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

Appendix 5: References

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

NHS Care Records Guarantee
http://systems.hscic.gov.uk/rasmartcards/strategy/nhscrg

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

The Health Service (Control of Patient Information) Regulations 2002
http://www.legislation.gov.uk/uksi/2002/1438/contents/made

Confidentiality Advisory Group
http://www.hra.nhs.uk/resources/confidentiality-advisory-group/

NHS Encryption Guidance
http://systems.hscic.gov.uk/infogov/security/infrasec/iststatements/dataenc_html

Caldicott Report
https://www.gov.uk/government/publications/the-information-governance-review

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

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