NHS
South Devon and Torbay
Clinical Commissioning Group

NHS SOUTH DEVON AND TORBAY CLINICAL COMMISSIONING GROUP AND NHS NORTHERN EASTERN & WESTERN DEVON CLINICAL COMMISSIONING GROUP

CONFIDENTIALITY AND DATA PROTECTION POLICY

Version: 2.2 dated 15 November 2017

Version Control

DATE	VERSION	CONTROL
08/02/2013	1.0	First draft of new data protection policy - Jenna Ray
17/04/2013	1.0	Additions to include data sharing with the HSCIC and Section 251 arrangements.
24/04/2013	1.1	Expand policy to include all aspects of Confidentiality as well as Data Protection.
26/06/2013	1.1	Approved by SDT CCG Quality Committee
17/07/2015	2.0	Policy reviewed with minor amendments made: Page 7 added ID badge access and reference to Iron Mountain. Principle 7 to Appendix 2. Page 8 - Pseudonymisation paragraph added. 3.9.2 - Short paragraph added regarding audits of the N Drive
09/09/2015	2.0	Approved by Quality Committee
14/11/2016	2.1	Removed reference to NHS Connecting for Health 4.8.1 - Amended IG training wording 3.3.4 and 3.7 - Updated Records Management Code of Practice Updated several footnotes
24/01/2017	2.1	Approved by IG Forum
09/03/2017	2.1	Approved by Quality Committee
15/11/2017	2.2	Amended to include NEW Devon CCG

South Devon and Torbay Clinical Commissioning Group and Northern Eastern & Western Clinical Commissioning Group promotes equality, diversity and human rights and is committed to ensuring that all people and communities it serves have access to the services we provide. In exercising the duty to address health

inequalities, the CCG has made every effort to ensure this policy does not discriminate, directly or indirectly, against patients, employees, contractors or visitors sharing protected characteristics of: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion and belief; sex (gender); sexual orientation or those protected under Human Rights legislation. All CCG policies can be provided in large print or Braille formats; translations on request; language line interpreter services are available; and website users can use contrast, text sizing and audio tools if required. For any other assistance, please contact the SD&T CCG at sdtccg@nhs.net or 01803 652500

CONTENTS

1 Purpose

This policy provides reference and guidance to follow by legal obligations, as outlined by the Data Protection Act 1998 and other legislation.

2 Executive Summary

The CCG processes information about individuals including patients and staff. As an organisation, we are therefore required to comply with the Data Protection Act 1998. As a part of the NHS, we are obligated to follow the NHS Confidentiality Codes and also comply with the Caldicott Principles. As an employer we have obligations of confidentiality and under data protection principles concerning our staff.

This Data Protection Policy aims to detail how the CCG meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998. It includes such activities as patient administration/payment, employee and staff administration, purchasing, invoicing and treatment planning, payroll and the use of manual records relating to individuals whose information may be held within the organisation. This list is not exhaustive.

Each of the teams and employees within the organisation has a duty under the Act to hold, obtain, record, use, and store all personally identifiable information necessary to perform their role in a secure and confidential manner. All processing of personal data by, or on behalf of the organisation must be in accordance with the eight Data Protection Principles, a summary of which is set out in Appendix 1. In addition, for patient data, the Caldicott Principles should also be followed, a summary of which is set out in Appendix 2.

3 Introduction

The Data Protection Act 1998 ("the" Act) regulates the "processing" (which broadly means the obtaining, using, holding and disclosing) of data relating to individuals. "Data" includes automated or computerised data, and also manual files and records forming part of a "relevant filing system" which loosely means a structured set of paper records from which one can readily extract particular information on an individual. The Act also covers "accessible records" including health records. The Act only applies to living people, although the requirements of the Access to Health Records Act 1990, which covers both living and deceased patients, are also applicable to the CCG.

3.1 Overview of Legislation

The legislation listed below also refers to issues of security and/or confidentiality of personal identifiable information/data.

Police and Criminal Evidence Act 1984[1]
Access to Medical Reports Act 1988[2]
Access to Health Records 1990[3]
Data Protection Act 1998[4]
Human Rights Act 1998[5]
Crime and Disorder Act 1998[6]
Freedom of Information Act 2000[7]
Regulation of Investigatory Powers Act 2000[8]
Health and Social Care Act 2001[9]
NHS Act 2006[10]
Health and Social Care Act 2012[11]

3.2 Data Protection Act 1998

This Act applies to all personally identifiable information held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays etc.

The Act dictates that information should only be disclosed on a need to know basis, for

[1] Police and Criminal Evidence Act 1984 http://www.legislation.gov.uk/ukpga/1984/60/contents
[2] Access to Medical Reports Act 1988 http://www.legislation.gov.uk/ukpga/1988/28/contents
[3] Access to Health Records 1990 http://www.legislation.gov.uk/ukpga/1990/23/contents
[4] Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
[5] Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents
[6] Crime and Disorder Act 1998 http://www.legislation.gov.uk/ukpga/1998/37/contents
[7] Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents
[8] Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents
[9] Health and Social Care Act 2001 http://www.legislation.gov.uk/ukpga/2001/15/contents
[10] NHS Act 2006 http://www.legislation.gov.uk/ukpga/2006/44/contents
[11] Health and Social Care Act 2012 http://www.legislation.gov.uk/ukpga/2012/7/contents

legitimate reasons connected with the CCG's business or through a defined legal requirement. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

The Act also requires the CCG to register its data holdings with the Information Commissioner's Office, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. The CCG also has to comply with the principles of good practice known as the eight Data Protection Principles (Appendix 1). From April 2010 the Information Commissioner has the power to fine data controllers up to £500,000 for contravening data protection principles likely to cause substantial damage or distress.

All applications and databases required under law to be registered for Data Protection purposes will be registered in general terms under the CCG's registration with the Information Commissioner and will comply with the Data Protection Act 1998.

Under section 7 of the Data Protection Act an individual can request access to their personal data held by the CCG. The CCG will process all requests received in line with the Act.

3.3 NHS Guidance

3.3.1 Confidentiality: NHS Code of Practice. November 2003[12]

The Code's purpose is to provide guidance to the NHS and NHS related organisations on patient information confidentiality issues. It also considers ways of obtaining and using patient information to comply with Data Protection legislation, current and planned.

3.3.2 Supplementary Guidance: Public interest disclosures. November 2010[13]

This document expands upon the principles set out with the Department of Health's key guidance Confidentiality: NHS Code of Practice. The document is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest.

3.3.3 Information Security Management: NHS Code of Practice. April 2007[14]

A guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice.

3.3.4 Records Management: Code of Practice for Health and Social Care. July 2016[15]

This Code is a key component of information governance arrangements for the NHS. It sets out the required standards of practice in the management of records for those who work

[12] Confidentiality: NHS Code of Practice. November 2003
http://systems.digital.nhs.uk/infogov/codes/confcode.pdf
[13] Supplementary Guidance: Public interest disclosures. November 2010
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/152224/dh_122031.pdf.pdf
[14] Information Security Management: NHS Code of Practice. April 2007
http://systems.digital.nhs.uk/infogov/codes/securitycode.pdf
[15] Records Management: Code of Practice for Health and Social Care. July 2016
http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.

3.4 Data Protection Principles

There are eight principles of good practice within the Data Protection Act 1998. These are normally referred to as the 'data protection principles'. A summary of these are shown in Appendix 1. An overview of these principles as they apply to the CCG is shown below:

3.4.1 Fair Obtaining/Consent

There is a requirement to make the general public, who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The CCG is obliged under the Data Protection requirements and Caldicott recommendations to produce patient information leaflets and posters which are customised to its own use/s of patient information. In practice the CCG does not use patient data for purposes other than investigating incidents arising from primary and secondary care, plus the uses allowed under section 251 of the NHS Act 2006.[16] A Fair processing Notice (FPN) is published on the CCG's website.

3.4.2 Staff

There must also be procedures to notify staff, temporary employees (volunteers, locums) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed. This may occur during induction or by their individual manager.

3.4.3 Patients

Patients will be made aware of this requirement by the use of information posters in patient waiting areas, statements in patient handbooks/on survey forms and verbally by those health care professionals providing care and treatment. Patient information leaflets and posters will be produced as required for specific purposes and made available in the relevant patient areas in primary and secondary care across the CCG.

3.5 Data Protection Notification

The Data Protection Act 1998 requires every data controller who is processing personal information to notify, unless they are exempt[17]. The CCG will notify the Information Commissioner's Office of its data processing intentions and the subsequent registration will be renewed annually. All registrations can be viewed online via a publicly available register held by the Information Commissioner's Office, see www.ico.gov.uk. The SD&T CCG's registration number is Z352563X and NEW Devon CCG's registration number is Z3602533.

3.6 Accuracy/data quality

The CCG has to ensure that all information held on any media is accurate and up to date. The Data Quality Group will check that accuracy of information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users. Users of software will be responsible for the quality (i.e. Accuracy, Timeliness, and Completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

[16] National Information Governance Board http://www.nigb.nhs.uk/advice/quickrefguideinfomat
[17] Data Protection Act 1998, section 18, 19 http://www.legislation.gov.uk/ukpga/1998/29/contents

Staff should check with patients that the information held by the CCG is kept up to date by asking patients attending appointments to validate the information held.

3.7 Retention of data

All records are affected by this procedure regardless of the media they may be held, stored, retained. The Information Governance Alliance's "Records Management – Code of Practice for Health and Social Care"[18] and NHS England's Retention Schedule and Disposal Guidance provides comprehensive guidance for CCGs.

The fifth data protection principle makes it clear that data should not be kept for longer than necessary. Where "clear" data (i.e. patient identifiable) is processed by the CCG it should be held in clear form for as short a time as possible. Clear data should be pseudonymised or anonymised before use wherever possible.

For further guidance please refer to SD&T CCG's Information Lifecycle Management Policy.

3.8 Individual's rights – including subject access/right to complain

Under this principle of the Data Protection Act individuals have the following rights:

- right of subject access (section 7)
- right to prevent processing likely to cause harm or distress (section 10)
- right to prevent processing for the purposes of direct marketing(section 11)
- right in relation to automated decision taking (section 12)
- right to take action for compensation if the individual suffers damage (section 13)
- right to take action to rectify, block, erase or destroy inaccurate data (section 14)
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened (article 28 of the Data Protective Directive)[19]

3.8.1 Subject Access Requests

Individuals have a right to apply for access to health, employment and other type of information held about them on computer and indexed paper records. These requests are made under the provisions of the Data Protection Act and the following points should be considered.

- Responsibility for dealing with a subject access request lies with the "data controller".
- Requests have a legal time limit of up to 40 days in which to respond.
- Any requests must be in writing and most cases the maximum fee that can be charged is £10.

When responding to a request, the individual must be:

- Told whether any personal data is being processed.

[18] Records Management: Code of Practice for Health and Social Care. July 2016
http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

[19] Data Protection Directive
http://www.ico.org.uk/about_us/research/~/media/documents/library/Data_Protection/Detailed_specialist_guides/REVIEW_OF_EU_DP_DIRECTIVE_SUMMARY.ashx

- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the information comprising the data.
- Given details of the source of the data (where this is available).

The data controller is the legal entity that determines the purposes for which and the manner in which personal data is processed. The SIRO or Caldicott Guardian for the CCG will verify and authorise all disclosures.

The Information Governance Lead is responsible for handling Subject Access Requests pertaining to patients and staff, and to ensure that systems and processes are in place to handle Subject Access Requests within the requirement of the Act..

3.8.2 Compensation

Individuals have a right to seek compensation from the relevant data controller for any breach of the Act which may cause them damage and/or distress[20].

3.8.3 Complaints

The CCG's complaints procedures take account of complaints which may be received because of a breach or suspected breach of the Data Protection Act 1998.

3.9 Security

All information relating to identifiable individuals must be kept secure at all times. The CCG will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Details of this are within the Information Security Policy.

CCG staff must report without delay to the information governance inbox d-ccg.informationgovernance@nhs.net any breaches. Incidents assessed as level 2 will be reported to the Information Commission's Office. A register will be maintained by the Information Governance team and, if required, recorded within the CCG Annual Report. Further details are contained in the Information Security Policy.

3.9.1 Physical security measures in place within the CCGs include:

- Secure access to the CCG's offices at Pomona House. The CCG's main entrance and further two doors are restricted to CCG ID badge holders only. NEW Devon CCG have a manned reception during working hours and at other times and other entrances coded locks
- Paper records are held in locked cabinets / drawers in the main office. Archived records are maintained by Iron Mountain. NEW Devon CCG archived records are managed and controlled by Crown Records Management. A clear desk policy mandates nothing is to be left unattended and items to be locked away securely in lockable cabinets.
- Confidential paper waste is shredded to DIN32757-1 level 4 standard before leaving the office.

3.9.2 Electronic security measures in place within the CCG include:

- All software and data is removed from redundant hardware and media storage (e.g. CDs, disks) before the hardware is removed from the South Devon Health

[20] Data Protection Act 1998, section 13 http://www.legislation.gov.uk/ukpga/1998/29/contents

Informatics Service (HIS), who provide IT support to SD&T CCG. For NEW Devon CCG this service will be performed by Delt who provide IT support.

- All IT equipment issued to the CCG is encrypted.
- The CCG undertakes annual audits of its electronic data storage (the N Drive) to ensure that staff only have access to the information they require to carry out their role. This also ensures that any patient confidential data is kept secure and is used/stored for its intended purposes only.

3.9.3 Disclosure of information/information in transit

It is important that information about identifiable individuals (such as patients and staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

Some disclosures of information may occur because there is a statutory requirement upon the CCG to disclose e.g. with a Court Order, or because other legislation requires disclosure (tax office and pension agency for staff and notifiable diseases for patients).

If person identifiable information/records need to be transported in any media NHS encrypted memory sticks (available from the HIS and Delt) must be used to maintain strict security and confidentiality of this information. If paper records are being transported refer to Information Security Policy.

Reliable transport couriers should be used at all times – for example, the Department of Health currently recommend TNT couriers. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturer's specifications. Contracts between the CCG and third parties should include an appropriate confidentiality clause which should be disseminated to the third parties employees.

3.9.4 Patient Information

There are specific requirements highlighted within the Caldicott principles[21] that apply to patient identifiable information. Most of these are also requirements of compliance with the Data Protection legislation. Specifically they relate to security, confidentiality and fair obtaining of information as well as ensuring all disclosures are valid and authorised. All patient information, whether held manually or automatically, will be kept secure when not being used for patient care or related purpose.

The CCG receives pseudonymised patient information from the Data Services for Commissioners Regional Office (DSCRO) South West for non-direct care purposes. The CCG needs to plan and commission healthcare services in its local area through analysis of actual and projected use of services across all parts of the care economy. This modelling requires access to information about care provided to patients, their hospitals stays and patient journeys but without accessing personal confidential patient data. This service allows the CCG to plan and commission those healthcare services in its local area using the services provided through the DSCROs.

4 Roles and Staff Responsibilities

Every member of staff, whether employed, self-employed, consultant, locum, contractor or

[21] Caldicott Principles http://systems.digital.nhs.uk/infogov/links/cald2rev.pdf

agency, has individual responsibility for compliance with this policy and the requirements of the Act. The following roles have additional responsibilities as set out below. Failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action. In some cases, serious breaches such as unlawful obtaining or disclosure of personal information may result in criminal prosecution.

4.1 Chief Clinical Officer

The Chief Clinical Officer of NHS SD&T CCG and NEW Devon CCG has overall responsibility within the organisation for compliance with data protection requirements. The development, implementation of, and compliance with this policy is delegated to the Caldicott Guardian, Senior Information Risk Officer and the Information Governance Lead, whose details are set out below.

4.2 Caldicott Guardian

The Caldicott Guardian is an appropriately qualified and trained senior health professional appointed as a guardian, responsible for safeguarding the confidentiality of patient information. In conjunction with the Senior Information Risk Owner (SIRO) the Caldicott Guardian will oversee all disclosures of individual personal information with particular attention being paid to extraordinary disclosures.

The Chief Nursing Officer is currently the Caldicott Guardian for both CCGs.

4.3 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) for NHS South Devon & Torbay CCG is the Joint Director of Primary Care, South Devon & Torbay and NEW Devon CCGs and for NEW Devon CCG is the Chief Financial Officer. The SIRO will ensure that the Senior Management Team and Chief Clinical Officer of NHS South Devon & Torbay Clinical Commissioning Group and NEW Devon CCG are kept up to date and briefed on all Information Governance and Information Security issues affecting the organisation.

- To ensure appropriate notification in compliance with the Data Protection Act is maintained.
- Dealing with enquiries about data protection issues.
- Advising and training staff on their data protection responsibilities in conjunction with the Caldicott Guardian and the Legal Team, responsibility for advising on actual or potential breaches of confidentiality, and recommending remedial action.
- Ensuring the organisation has an action plan for achieving Data Protection related requirements within the NHS Digital IG Toolkit.
- Ensuring the organisation has procedures in place to comply with relevant Department of Health best practice guidance such as Confidentiality and Records Management code of practice.
- Liaising with external organisations on data protection matters.
- The development and implementation of information sharing protocols.
- Oversee all disclosures of individual personal information.

4.4 Information Governance Forum

The Information Governance Steering Group for NHS SD&T CCG & NEW Devon CCG is chaired by the SIRO and supported by the Information Governance Lead. The Information Governance Steering Group has the following responsibilities:

- monitoring Information Governance Toolkit submissions across the CCG.
- ensuring that policies are developed and updated in line with legislation, contractual requirements and NHS requirements, as updated from time to time.
- identifying any new information (e.g. national guidance, staff or patient feedback) that may trigger review and amendment of policies before the due date.
- identifying individuals and groups who must be aware of/work within the confines of this policy and agreeing appropriate dissemination.
- advising on training requirements.
- ensuring that sufficient resources are provided to support the requirements of the policy and on-going Information Governance agenda.

4.5 Information Governance (IG) Lead

The IT & IG officer at NHS South Devon & Torbay Clinical Commissioning Group will act as the IG Lead with the IG Manager acting as the IG Lead at NEW Devon CCG. The role of the IG Lead includes:

- overseeing the policies and procedures required by the Act and subsequent regulations, NHS requirements and the Caldicott Principles.
- reviewing the CCG's Data Protection registration.
- acting as first point of contact for training, advice and support for all staff on matters relating to Information Governance and Data Protection which may arise within the relevant company.
- Managing the Information Governance Toolkit submissions.

4.6 Line Managers

Managers will ensure that all staff including contractors, bank, voluntary and other agency staff:

- are instructed in their security and Data Protection responsibilities and attend Information Governance training specific to their job role.
- are trained in the secure use of using computer systems/media.
- are aware of their data protection obligations, this policy and associated procedures /guidelines and any updates.
- are able to identify and know how to deal with subject access and Freedom of Information requests.
- know how to access and store personal identifiable information, both in manual and electronic records.
- ensure no unauthorised staff are allowed to access any computer system utilised by the organisation.
- ensure access control of all staff as described within the Information Security Policy.
- ensure current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability.

4.7 All Staff

Every member of staff (including agency, bank, locums, volunteers, contractors, non-contract and student placements) will in the course of their work, handle and/or be in contact with confidential and/or personal information whether relating to staff, patients or their carers, business, family or friends or any other individuals connected to the organisation in some way.

All staff are required to:

- be made aware of and adhere to this policy, associated procedures/guidelines and all related systems and processes.
- attend data protection (or relevant Information Governance) training as appropriate.
- ensure that all personal identifiable information is accurate, relevant, up to date and used appropriately, both electronic and manual records including the use of databases.
- ensure that all person identifiable information is kept safe and secure at all times.
- have signed a contract of employment, a contract for services or a non-disclosure agreement (as applicable) that includes Confidentiality, Information Security and data protection clauses.
- understand that breaches of this policy will be investigated by formal disciplinary procedure (or contractual enforcement if appropriate) which may lead to dismissal and/or legal action.

Staff should also ensure that they keep their HR information up to date and notify the relevant HR team or their line manager of any relevant changes.

4.8 Staff Issues

4.8.1 Training

The CCG will ensure that all staff are aware of the policies and requirements regarding data protection and appropriate training arrangements will be made available via ESR and bespoke in-house training relevant to team's and individual's needs.

4.8.2 Induction

All CCG staff will receive Information Governance training as part of the overall induction process.

4.8.3 Contracts of Employment

All CCG staff, contractors, temporary employees and volunteers will sign contracts that specify data protection, information governance and information security expectations and obligations.

4.8.4 Disciplinary

A breach of the Data Protection requirements could result in a member of staff facing disciplinary action. Copies of these procedures are available from the Human Resources Department.

4.9 Monitoring and Audit of this policy

This policy and associated appendices and procedures will be monitored by the Information Governance Steering Group. It is also expected that both Internal and External Audit will review this and associated policies and procedures.

4.10 Staff Information

Any member of staff current, past or potential (applicant) who wishes to have a copy of their employment information under the subject access provision of the Data Protection Act will need to contact, in writing, the Data Protection Lead of the CCG. There are subject access procedures outlining the process to follow to deal with such requests.

5 Conclusion

This Data Protection Policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 but takes into account other legislation covering security and confidentiality of personal information.

Appendix 1

Data Protection Principles

There are eight principles of good practice within the Data Protection Act 1998[22]. These are normally referred to as the 'data protection principles'.

1) **Personal data shall be processed fairly and lawfully.**

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

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

4) **Personal data shall be accurate and, where necessary, kept up to date.**

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

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

7) **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.**

8) **Personal data shall not be transferred to a country or territory outside the EU 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.**

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

Appendix 2

Caldicott Principles[23]

1) **Justify the Purpose.**

2) **Don't use patient identifiable information unless it is absolutely necessary.**

3) **Use the minimum necessary patient-identifiable information.**

4) **Access to patient identifiable information should be on a strict need-to-know basis.**

5) **Everyone with access to patient identifiable information should be aware of their responsibilities.**

6) **Understand and comply with the law.**

7) **The duty to share information can be as important as the duty to protect patient confidentiality.**

[23] Caldicott Principles http://systems.digital.nhs.uk/infogov/links/cald2rev.pdf