

**DOCUMENT CONTROL PAGE**

<b>Title</b>	<b>Title: Data Protection Policy</b> <b>Version: 4</b> <b>Reference Number:</b>
<b>Supersedes</b>	<b>Supersedes: Data Protection Policy v.3 November 2006</b> <b>Significant Changes: Updated to reflect changes in procedure</b>
<b>Originator or modifier</b>	<b>Originated By: Cara Taylor</b> <b>Designation: Data Protection &amp; Freedom of Information Manager</b> <b>Modified by: Nicholas Jones</b> <b>Designation: Data Protection &amp; Freedom of Information Manager</b>
<b>Ratification</b>	<b>Referred for approval by: Information Governance Group</b> <b>Date of Referral: 21 January 2011</b>
<b>Application</b>	<b>All staff</b>
<b>Circulation</b>	<b>Issue Date: January 2011</b> <b>Circulated by: Information Department</b> <b>Issued to: All staff via intranet</b>
<b>Review</b>	<b>Review Date: January 2014</b> <b>Responsibility of: Head of Information and Analysis</b>

<b>Date placed on the Intranet:</b>	<b>Please enter your EqIA Registration Number here:</b> <b>195/11</b>  <b>Refer to section 5: Equality, Diversity and Human Rights Impact Assessment</b>
-------------------------------------	---

Section	Contents	Page
1	Introduction	
2	Purpose	
3	Roles and Responsibilities	
4	Detail of Policy	
5	Equality, Diversity and Human Rights Impact Assessment	
6	Consultation, Approval and Ratification Process	
7	Dissemination and Implementation	
8	Monitoring Compliance of Procedural Documents	
9	References and Bibliography	
10	Associated Trust Documents	
11	Appendices	

## 1 Introduction

- 1.1 This policy sets out how the Trust will meet the requirements of the Data Protection Act 1998 (DPA), which details how personal data should be processed. This policy applies to all permanent, temporary, honorary and contracted staff, as well as students and those on work experience who have access to information within the Trust. The policy should be followed whilst working for the Trust and also after employment has ended.
- 1.2 Any employee who breaches the standards of this policy may be subject to disciplinary action, in accordance with the Trust's disciplinary procedures. This could result in summary dismissal for gross misconduct. Separately to this, use or disclosure of personal data which is outside of this policy could be a criminal offence.

## 2 Purpose

- 2.1 This policy provides guidance on how personal data must be handled to ensure compliance with the relevant legislation and codes of practice.

### 3 Roles and Responsibilities

- 3.1 The **Chief Executive** has overall responsibility and accountability for Data Protection and is required to provide assurance, through the statement of internal control, that all risks relating to information are effectively managed and mitigated.
- 3.2 The **Caldicott Guardian (Medical Director)** has overall responsibility for ensuring that all personal data is stored and used in accordance with the Data Protection Act 1998 and the Caldicott Principles.
- 3.3 The **Director of Informatics** is the **Senior Information Risk Owner (SIRO)** and acts as an advocate for information risk on the Trust Board.
- 3.3.1 **The Head of Information will maintain the Trust's notification with the Information Commissioner and be the contact for any breaches of this policy. Breaches will be reported to the SIRO or Medical Director.**
- 3.4 The **Data Protection and FOI Managers** will deliver training sessions on the DPA, including at Trust Corporate Induction and will be the first point of contact for any Data Protection or confidentiality queries. They will be the contact point for external agencies and will maintain a log of all systems containing personal data.
- 3.5 The **Head of Medical Records** will oversee subject access requests for medical records and ensure they are dealt with in line with the Access to Health Records Policy.
- 3.6 Line Managers will handle subject access requests for copies of personnel files. They will also be responsible for ensuring that this policy is adhered to in their area of responsibility and must ensure that staff in their area are aware of the Policy and their responsibilities.
- 3.7 All employees, bank staff, agency staff, volunteers and contractors must comply with this policy.

### 4 Details of Policy

#### 4.1 Principles

The DPA sets out eight principles for the processing of personal data. These must be followed at all times.

- 4.1.1 **One: Personal data will be processed fairly and lawfully.** Any use of personal data must comply with all relevant rules of law, for example the Human Rights Act 1998, and relevant conditions in schedules two and three of the DPA must be met. Use of personal data will be deemed fair if the

<i>Data Protection Policy</i>	<i>Page 4 of 18</i>
<i>See the Intranet for the latest version.</i>	<i>Version Number:- 4</i>

individual the information relates to has been informed what is held and how that information will be used, for example whether disclosures will be made. The trust has a fair processing notice for patients in the leaflet 'Your Information' which is available in all patient areas. Replacement copies can be requested from the printing department.

- 4.1.2 **Two:** Personal data will be obtained for specified and lawful purposes and will not be used in a way which is unsuited to those purposes. This looks at the understanding which the individual had when they provided their personal data. They should not be surprised by the ways in which that data is subsequently used, and staff should communicate any changes to the way information is used to patients and seek their consent.
- 4.1.3 **Three: Personal data will be adequate, relevant and not excessive for the purposes for which it is used.** This means that a data controller must hold the minimum amount of data which is needed, and should always assess whether it is necessary for data to be held. Irrelevant data should not be collected.
- 4.1.4 **Four: Personal data will be accurate and up to date.** Data controllers must make sure that reasonable steps are taken to record accurate personal data. If information is factually inaccurate it must be amended. When information consists of an opinion or personal recollection of events it can not usually be proven to be inaccurate and so an individual's objections to such subjective information should be recorded. Information which is subject to change should be checked at reasonable intervals.
- 4.1.5 **Five: Personal data will not be kept for longer than is necessary.** Information should be reviewed regularly to assess whether it is still needed. Deletion or destruction should be in line with the Trust's retention policy which is available on the intranet. As an example, it may be that some information from an individual's personnel file will be deleted before the rest, to ensure that only the necessary information is retained – for legal reasons or in order to provide a reference for example.
- 4.1.6 **Six: Personal data will be processed in line with individuals' rights.** Under the DPA data subjects have the following rights:
- right of access to personal data (through a subject access request)
  - right to object to processing that is likely to cause or is causing damage or distress;
  - right to prevent processing for direct marketing;
  - right to object to decisions being taken by automated means;
  - right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
  - right to claim compensation for damages caused by a breach of the Act.
- 4.1.7 **Seven: Appropriate technical and organisational measures will be taken to protect against unauthorised or unlawful processing, accidental loss, destruction or damage to personal data.** The Trust has to consider the

possible consequences should each type of data be unprotected and put in place a level of security which reflects this risk. The Trust also has to ensure that staff are reliable and aware of how to protect the data they are dealing with. This principle sets down that, when employing outside companies to process personal data, those companies must be under contract. This contract will outline the ways in which the data should be used and provide no autonomy to the outside company. If there is any autonomy about how the information is used, the contracting company will also be data controllers for the information.

**4.1.8 Eight: Personal data will not be transferred to a country which does not have adequate levels of protection for the information.** Any countries within the European Economic Area (EEA) (the EU plus Iceland, Liechtenstein and Norway) are subject to data protection legislation and so deemed adequate. The European Commission has also decided that the following are adequate for transfers:

- Andorra;
- Argentina;
- Canada;
- Guernsey;
- Isle of Man;
- Israel;
- Jersey;
- Switzerland;
- United States (under the Safe Harbor scheme only).

**4.1.9** If you wish to transfer personal data to a country which does not have adequate protections, either the consent of each of the individuals must be sought before transferring their data or a contract must be set up between this Trust and the other organisation. You must contact the Data Protection and Freedom of Information Manager for further information.

**4.2 The Caldicott Principles** relate to the use of patient identifiable data in the NHS and should be followed at all times. The principles are as follows:

**4.2.1 One:** Justify the purpose for using personally identifiable information.

**Two:** Only use personally identifiable information if absolutely necessary.

**Three:** Use only the minimum data needed for the specific purpose.

**Four:** Restrict access to information only to those who need to know.

**Five:** Individuals should be aware of their responsibilities to keep data confidential.

**Six:** Individuals should understand and comply with the law.

### **4.3 Anonymisation**

Information is only classified as personal data if it identifies an individual. Therefore information which has been stripped of identifiers will not be covered by the DPA. To comply with the third DPA principle (processing

should not be excessive) and the second Caldicott principle, anonymised, de-identified or pseudonymised data should be used wherever appropriate.

- 4.3.1 For information to be truly anonymous there should be no way of linking that information to an individual. For example, if a database contains clinical information along with names and addresses or even just the postcode and date of birth, this will be personal data. Information relating to an individual with a rare condition could also identify them without naming them and therefore usual methods of anonymisation may not always be appropriate. If information about the number of referrals made by one hospital was requested by another Trust, there would be no need to name the patients or include any other identifiers along with the statistics. The anonymised list would not be personal data in the hands of the receiver but it would be in the hands of this Trust as it is possible to link that information to individuals.

#### 4.4 Access to information

- 4.4.1 This section should be read together with the Access to Health Records policy.
- 4.4.2 Section seven of the DPA gives everyone the right to access personal data that is held about them, and to be told what it is used for and who it is given to. Individuals also have the right to receive a copy of their own personal data.
- 4.4.3 Any request for a copy of personal data must be made in writing (this includes letters, faxes and emails). The Trust has a form to be completed, and is entitled to request further information in order to:
- 4.4.4 Identify the individual making the request.
- 4.4.5 Be satisfied that they have the appropriate authorisation if making the request on behalf of another;
- 4.4.6 Locate the information which has been requested.
- 4.4.7 A fee can be charged for providing the information. If the information which has been requested consists of health records, a maximum of £10 can be charged for provision of any information held on computer. If any or all of the information is held manually – in paper file – a maximum of £50 can be charged. Information which is not a health record must be provided for a maximum of £10 no matter how it is held.
- 4.4.8 Once the necessary information and the fee have been received the Trust legally has 40 calendar days to provide the information which has been requested. The Department of Health recommends that

information should be provided within 21 calendar days as good practice.

- 4.4.9 Requests for medical records should be directed to the Medico-Legal team. Requests for staff records should be referred to the relevant line manager.

#### 4.5 Third Party Information

- 4.5.1 A third party is any individual other than the person the data is primarily about. If the information which has been requested includes information which relates to third parties, consideration must be given to whether the identities of the third parties can be edited out. If this is not possible, either because the individual would still know who the information was about or the information would not make sense without those identities, the Trust must consider asking the third party for their permission to disclose the information. If this request is refused, it must be considered whether it is reasonable in all the circumstances to disclose the information without consent. This decision must balance the effect on the individual of withholding the information against the possible loss of confidentiality by the third party. In most cases the emphasis should be on facilitating disclosure.
- 4.5.2 The name of a member of staff acting in their professional capacity would not usually be seen as requiring protection. However, there are circumstances where the identity of a member of staff may have been recorded in confidence and therefore this would be treated differently – for example, the name of a staff member making a complaint may be withheld. This would depend on the specifics of each case.
- 4.5.3 If a decision is made to withhold information the Trust is not obliged to provide the reason (note that this differs from the Freedom of Information act where any exemptions must be fully explained to the requester). However, in most cases it is helpful to explain why information has been withheld, unless this is in itself sensitive.

#### 4.6 Medical records

- 4.6.1 When a request is received for a copy of information about an individual's health, which that individual has not previously seen and which could cause harm to their physical or mental health, the relevant health professional must be consulted. The relevant health professional will be the person who is responsible for the clinical care of the individual. If the individual has not been a patient for some time and the professionals who treated them have since left the Trust, the most appropriate health professional must be consulted. This health professional will then decide whether any of the information would be of detriment to the physical or mental health of the individual or any other person. If this is the case, the harmful pieces of information should be removed from the copies provided. Access to the records may be refused in exceptional cases.

4.7 An individual has a right to view their manual health records free of charge if they were added to in the last 40 calendar days before the request was made. The above processes for considering the removal of third party information or requesting a health professional's opinion would have to be followed before the individual viewed the records. The patient must not be left alone with the records at any time. Care should be taken to ensure the security of the original records. In addition to the above, this Trust allows any patient to view their health records – even if they were not added to in the last 40 calendar days. No charge is made for this service. Please see the Access to Health Records policy for full details of the procedure for viewing records

#### 4.8 Requests from third parties

4.8.1 If a subject access request is received from another person on behalf of a patient it is necessary to ensure that the patient has authorised them to receive the information. For example, an individual may be acting on behalf of a relative, a solicitor on behalf of a client, or a trade union representative on behalf of a member. There is a section of our subject access forms which allows a patient to give this authorisation. The third party will then have the same rights as the patient and should be given any information the patient would be given.

4.8.2 Solicitors and insurance companies should only be requesting information which is relevant to their case or claim. If a full file has been requested, the company should be asked, if appropriate, to narrow down their request to relevant information – for example any treatment as a result of a fall.

#### 4.9 Exemptions

4.9.1 The DPA sets out a number of exemptions which allow information to be withheld from the response to a subject access request. If you have any questions about the application of these exemptions please contact the Trust Data Protection and Freedom of Information Manager. The exemptions are as follows:

- Safeguarding national security.
- Crime and taxation
- Regulatory activity
- Literature, journalism and art
- Research, history and statistics
- Information made available to the public by or under any enactment
- References written by the Trust
- Armed forces
- Management forecasts / planning
- Negotiations
- Corporate finance
- Examination scripts and marks
- Legal professional privilege
- Self incrimination

- Exemptions contained within the data protection order 2000 (S.I. No. 419)
- Health order

#### 4.10 Information relating to the deceased

4.10.1 The Data Protection Act 1998 only applies to information about living individuals. Requests for health records which relate to a deceased person are dealt with under the Access to Health Records Act 1990. This Act provides a right to information to anyone who has a claim resulting from the person's death. In most cases this is a personal representative, executor or administrator of the will.

4.10.2 A fee of £10 along with posting and copying costs can be charged if the records were not added to in the last 40 calendar days. If additions were made in this time, the records should be provided free of charge. The information must be provided within 21 calendar days if the records were added to in the last 40 calendar days and within 40 calendar days if no additions were made in this time. Third party considerations must again be made before releasing such information. Only information created after 1991 has to be provided.

#### 4.11 Right to complain

4.11.1 Any individual who feels that information has been withheld from them will be asked to put their concerns in writing, outlining the information which they think is missing. If this is information which had been overlooked in error, it will be provided as soon as possible, once the original process of considering third party data or detriment to the individual has been followed. If the information was not requested originally because perhaps the existence of it has only just come to light through information which has been provided, the Trust will decide whether this can be provided free of charge or whether it must be viewed as a new request.

4.11.2 Should the information which is missing have been removed intentionally, either by the relevant health professional, because it contained third party information or another exemption applied, the Trust will respond to restate that they have been provided with all the information which they are entitled to. The Trust will provide information about the reason for removal where appropriate, and inform the individual of their right to seek an assessment of our decision from the ICO.

#### 4.12 Breaches of confidentiality

4.12.1 The unauthorised disclosure or use of personal data is a serious matter, and may result in disciplinary action by the Trust. This may also be a criminal offence under section 55 of the DPA. Health professionals may also be subject to action by their professional bodies.

4.12.2 The obligation to preserve the confidentiality of any information which relates to patients, staff or other Trust business remains indefinitely.

Data Protection Policy	Page 10 of 18
See the Intranet for the latest version.	Version Number:- 4

This means that even when you leave your employment with the Trust, you are still bound by the duty of confidentiality. You can not give out the information which you learned in your job at any time.

- 4.12.3 Any member of staff can disclose information reasonably and responsibly in the public interest where there is an instance of malpractice, under the Public Interest Disclosure Act 1998. Please refer to the Trust's 'whistle blowing' / Raising Concerns policy for further information.
- 4.12.4 Patients who feel their confidentiality may have been breached should be encouraged to contact the Patient Advice and Liaison Service (PALS).
- 4.12.5 When any member of staff recognises a situation where confidentiality is likely to be or has already been breached, line management must be advised, and an incident report completed. This can be done on the Trust's online reporting system which can be accessed through the intranet. More information is available in the Trust Wide Risk Management Strategy, available on the intranet.
- 4.12.6 Patients or employees who feel that their personal data has been used in a way which does not meet the data protection principles are encouraged initially to put their concerns in writing to the Trust's Data Protection and Freedom of Information Manager. If this proves unsatisfactory for the individual concerned they have the right to approach the ICO to ask for an advice or for an assessment.

#### 4.13 Giving out information without consent

- 4.13.1 While consent is generally necessary for the processing of personal data there are situations where disclosure without consent is appropriate. These include:
- When the information is needed for the purpose of legal advice or to assist in a legal case or potential legal case.
  - When the information has been requested under the Freedom of Information Act 2000 and none of the principles of the DPA would be breached by giving the information out. (Please see the guidance note on Disclosures of Staff Information for further details on this area).
  - When the information has been demanded by order of a court or has to be given out under any law or enactment.
  - The information is needed to prevent or detect a crime, to apprehend or prosecute an offender or to assess or collect any tax or similar duty.
  - It is in the vital interests of an individual – this is considered to be a life or death situation.

4.13.2 In the majority of these cases fair processing information must still be provided, meaning the individual should be informed of the disclosure.

#### 4.14 **Disclosing information by telephone**

4.14.1 Occasionally it will be necessary to divulge information over the phone and as long as it is clear the individual is entitled to it this is acceptable.

4.14.2 If a call is received from someone asking for information about a patient enough questions must be asked in order to be certain that they are entitled to the information. Information should only be given to the next of kin, and even then details should be limited.

4.14.3 Basic questions should be asked, such as asking the individual confirm their address and date of birth. If you have any concerns at all, you should take the callers number and offer to ring them back. This will give you the opportunity to check whether the caller's details and phone number are listed on the patient's records as the next of kin. If they are not, you can call them back and explain that unfortunately, as they are not listed, you are unable to give them any information. This is so that patient confidentiality is preserved.

4.14.4 You may also be asked to confirm the details of an appointment to a patient over the telephone. Again, you should be aware in this situation and make sure that you have enough information to be satisfied you are dealing with the right person.

#### 4.15 **Security**

- 4.15.1 The seventh data protection principle creates a duty to ensure the security of personal data held by the Trust. All employees therefore need to take appropriate steps to ensure data is secure. This applies to both manual and electronic information.

#### 4.16 **Manual data**

- 4.16.1 All personal data being sent from one department to another must be transferred securely. The method will depend on the sensitivity of the information and should be determined by the area manager or supervisor.
- 4.16.2 When health records or similar documentation are carried from one department to another by trolley, the trolley must be taken into the ward or office. The trolley must not be left unattended. If it is not possible to take the trolley into the room, it must be left as near to the door as possible. The trolley should only be left with no one present to watch it for as little amount of time as possible. This will reduce the possibility of security risks.
- 4.16.3 Patients can transfer their own records between designated points (like inpatient areas) in the hospital but the records must be placed in a sealed envelope.
- 4.16.4 Health records must be returned to the Medical Records Library immediately after use. Records must not be transferred between designated areas (records libraries, inpatient areas and so on) without the knowledge and approval of the medical records department. The medical records department must track the location of the notes on PAS. Medical records must not be removed from hospital by a member of staff unless the patient is being transferred and the member of staff is going with them. In this case the medical records department would also need to be told so that they can track the notes on PAS.

#### 4.17 **Electronic data**

- 4.17.1 When faxing personal data to an outside organisation, it must be sent to and from a safe haven fax machine. When receiving personal data from an outside organisation by fax, you should ask that it be sent to a safe haven fax machine. A safe haven fax machine is one which is kept in a secure room, away from the general public. The room must be locked when unattended. If a safe haven is not available the fax good practice process must be followed. This involves using a cover sheet, ensuring the fax number is correct and checking that the fax has been safely received.

#### 4.18 **Accuracy**

- 4.18.1 In line with the Data Protection Act 1998 the Trust is required to maintain the accuracy of personal data.

- 4.18.2 All staff should therefore ensure they are careful when recording personal information and that details are checked with the individual. Inaccuracies can lead to serious problems such as incorrect treatment to a patient or a member of staff's wages going into the wrong bank account. Every care must be taken when inputting information on to Trust systems. Make sure that you are certain of all the information you input and check on any details which do not seem correct.
- 4.18.3 If an individual provides evidence that information we hold about them is factually inaccurate, we will amend the information. However if the incorrect information was relied upon for any care or treatment, we must ensure that the file reflects that incorrect information was previously held. It may be necessary to have evidence of the information which was previously in place if any legal dispute arises. Also the file should show accurately what information the health professionals have relied upon. If the individual disagrees with an opinion on their file, this can not be proven to be inaccurate. In such a case, the individual is entitled to have a note placed on the file which outlines what they think is incorrect. Please speak to the Medical Records Department for further advice.

#### 4.19 **Registering databases**

- 4.19.1 Any existing or new databases which contain personal data (both electronic and manual) must be registered with the DP and FOI Manager. The form to be filled in can be found here on the intranet or by contacting the Data Protection Manager – see 'contact details'.
- 4.19.2 The reason this form needs to be completed is so that we can make sure our notification with the ICO is up to date. This notification is a list of the types of information we process, what we use it for and who it is given to. It is also helpful from an audit or Freedom of Information point of view to have a record of all the information processed. Please see the Freedom of Information policy for further information on this area.
- 4.20 Information sharing protocols
- 4.20.1 The Trust should have protocols in place with all of the organisations with which it shares personal data. These protocols are like contracts where the information to be shared is described along with the reasons for sharing it and the ways in which the information will be used. Both parties have to sign the protocol.
- 4.20.2 Some of the protocols already signed are 'high level' protocols and allow a number of different information flows. Other protocols are more specific and apply just to one flow of information perhaps even for one occasion.

4.20.3 If individuals or departments are sending information outside the Trust they should check whether a protocol is in place. The Data Protection and Freedom of Information Manager has a list of all of the protocols in place.

#### 4.21 Taking information off site

4.21.1 Staff who take personal data off Trust premises (other than in transit) will be held responsible for that data. Members of staff must ensure that they have their manager's approval.

4.21.2 Personal data must not be left unattended and unsecured at any time. Staff who jeopardise the confidentiality of patients or others will be subject to disciplinary proceedings.

4.21.3 Every precaution must be taken to make sure that personal data is not viewed by any individuals who do not have authorisation.

4.21.4 Data must not be left on display or unattended in a vehicle unless this is unavoidable.

4.21.5 Staff must not automatically forward their emails outside of the Trust. If you require access to the Trust server when off-site, you must contact the Informatics Service Desk.

4.21.6 Information which patients have provided in order to receive care and treatment from this Trust should never be removed from the Trust for any other purpose. When accessing Trust systems from a remote site including your home, Trust information must not be saved on a non-Trust owned PC or device. Trust recommended devices must be used and these must be kept safe and secure. All personal data must be deleted from these portable memory devices as soon as possible.

4.21.7 Staff accessing the Trust network or systems from outside the Trust must adhere to the Trust Virtual Private Network Policy document and other Trust policies.

4.21.8 Information must be anonymised where possible when taking it off site.

#### 4.22 Research

4.22.1 In line with the first and second principles of the Data Protection Act 1998 (see page 2 for terms used within this policy) we can only use an individual's personal data for research if we told them when we collected their information. This is because an individual may not expect that the information they have provided in order to receive care and treatment would be used for research.

4.22.2 If an individual was not informed that their information would be used for research consent must be sought. This consent would have to be provided on

an 'opt-in' basis. This means that the individual would have to actively provide their consent, rather than relying on lack of response to a communication.

- 4.22.3 If consent is needed for a large collection of data, you can consult with the National Information Governance Board for Health and Social Care (NIGB), who may allow the common law duty of confidentiality to be set aside in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable (in accordance with section 251 of the NHS Act 2006).
- 4.22.4 If an individual has consented to the use of their information for research purposes, should you wish to use the information for a later research project which the individual would not have been able to foresee, you would have to write to the individual to explain the new research and to invite any objections. This would then be deemed fair.
- 4.22.5 Once it has been established that the information has been collected fairly, it may be kept indefinitely if:
- The data are not processed to support measures or decisions relating to particular individuals; and
  - The data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.
- 4.22.6 In this instance the information would not have to be provided in response to a subject access request provided that the results of the research, or any resulting statistics, were not available in a form which identified individuals.
- 4.22.7 You must contact the Research and Development office if you are planning to carry out a research project. This applies to any member of Trust staff or to anyone doing research on Trust premises or involving Trust patients.
- 4.22.8 Funded, unfunded and commercially funded work must all be notified to the Research and Development. The Research and Development office should be informed before the research begins and before you apply for the funding (where relevant).
- 4.22.9 All research must also have received a favourable ethical opinion from an appropriate research ethics committee before it can begin. Contact the Central Office for Research Ethics Committees [www.corec.org.uk](http://www.corec.org.uk) for details. A research ethics committee would have to agree to your research even if it has been approved by the NIGB.
- 4.22.10 Please see the Research and Development web-page for more detailed information.

#### 4.23 Clinical Audits

Data Protection Policy		Page 16 of 18
See the Intranet for the latest version.		Version Number:- 4

- 4.23.1 All health care professionals have to take part in regular clinical audits. This is a method of making certain of quality of care provided to patients and also allows us to measure our Trust's practice against 'Best Practice'.
- 4.23.2 Clinical audits tend to use smaller sample sizes than research. The information on audit forms or audit reports should not identify any individuals - whether staff or patients. If the information is collected directly from individuals their consent should be obtained and they should be informed that the information will be anonymised.
- 4.23.3 All audits must be registered with the Clinical Audit Department. Please see the Clinical Audit web-page for more detailed information.

## **5 Equality impact assessment**

- 5.1 Central Manchester University Hospitals NHS Foundation Trust is committed to promoting equality and diversity in all areas of its activities. In particular, the Trust wants to ensure that everyone has equal access to its services. Also that there are equal opportunities in its employment and its procedural documents and decision making supports the promotion of equality and diversity.
- 5.2 The initial Equality Impact Assessment (EqIA) has been scored at 25. This has been completed and submitted to the Equality and Diversity Department for 'Service Equality Team Sign Off'.
- 5.3 Please contact the Equality and Diversity Department if you have any queries on 0161 276 5651 or [equality@cmft.nhs.uk](mailto:equality@cmft.nhs.uk).

## **6 Consultation, Approval and Ratification Process**

- 6.1 The policy has been approved by the Information Governance Group.

## **7 Dissemination and Implementation**

- 7.1 The policy will be placed on the intranet and previous versions removed. The policy will also be distributed to all staff involved in handling FOI requests.

## **8 Monitoring Compliance of Procedural Documents**

- 8.1 Process for monitoring compliance
- 8.2 The Information Governance Group is responsible for monitoring compliance. This will be conducted on an annual basis.
- 8.3 The following will be monitored for compliance:
- Compliance with Data Protection Act Principles
  - Reported incidents involving Data Protection issues

8.4 An action plan will be put in place to address any shortfalls in compliance.

## 9 References

- Data Protection Act 1998
- Caldicott Report
- Access to Health Records Act 1990
- Freedom of Information Act 2000

## 10 Associated Trust documents

- Information Governance Policy
- Access to Health Records Policy
- Code of Conduct on Confidentiality