The Rotherham NHS
NHS Foundation Trust

DATA PROTECTION POLICY

VERSION 2.3 - APPROVED

Approved by the Health Informatics Steering Committee:-

Date Approved: 15/04/2009

Review Date: 14/04/2011

Owner: Scott Reid, Head of Information

Author(s): Bev Doane, Health Records Manager
Scott Reid, Head of Information
Susan Wake, Human Resources Adviser

Version	Date	Amendment History
1.0	2 April 2008	Initial Draft document
1.1	24 April 2008	Draft to Head of Information for comments
2.0	05 September 2008	Policy combined with Health Records Subject Access Policy
2.1	28 October 2008	Comments incorporated
2.2	08 January 2009	Feedback from IGSG incorporated
2.3	12 March 2009	Feedback from IGSG and revised approval mechanism incorporated

1. AIMS AND PURPOSE OF THE POLICY

1.1 The Rotherham NHS Foundation Trust is committed to compliance with the Data Protection Act 1998 ("the DPA") and will follow procedures that aim to ensure that all employees, contractors, agents, elected members, partners or other service providers of the Trust are fully aware of and abide by their duties and responsibilities under the DPA.

1.2 The Trust will ensure that personal data is handled, legally, securely, efficiently and effectively and in accordance with the eight principles of the Data Protection Act (**See Section 12 below**).

1.3 This Policy sets out the process for accessing both Health Records and Staff Records held by the Trust (**see Appendix 1 & 2**).

1.4 In order to operate efficiently the Trust will collect and use data relating to patients receiving care and the people with whom it collaborates including members of the public, current, past and prospective employees, suppliers and other visitors. In addition, it may be required by law to collect and use data in order to comply with the statutory requirements of the Department of Health, the Strategic Health Authority and other government departments.

1.5 All personal data, regardless of how it is collated, recorded, utilised and disposed of, whether on paper, by computer or other recording material, will be handled by the Trust within the safeguarding principles of the DPA and Information Governance frameworks issued by the Department of Health.

1.6 This Policy supersedes the ***Information Security & Confidentiality Policy*** and the ***Release of Health Records Policy***.

2. SCOPE OF THE POLICY

2.1 This Policy applies to all employees of the Trust, including Medical and Dental employees, contractors, agents, elected members, FT members, charitable groups, partners or other service providers of the Trust.

2.2 This Policy can be found in the Information Governance Policies section of the Trust's Intranet.

2.3 This Policy forms part of a framework of other information governance policies which can also be found on the Trust's Intranet (see section 8 for further details).

3. ROLES AND RESPONSIBILITIES

3.1 <u>All Employees</u>

Employees are responsible for ensuring that this Policy (**and related policies in section 8**) is followed.

3.2 Employees must ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that personal data is kept:-

- In a safe place where there would be no unauthorised access, and must not be left unattended in public/waiting areas
- In a locked filing cabinet or drawer where possible
- In an office with restricted access, or
- On disk, memory stick or other electronic storage system, appropriate security measures must be used (contact the IT helpdesk for further information)

3.3 Employees must:-

- Check that any personal data they provide to the Trust is accurate and up to date
- Ensure data provided by and recorded for others (i.e. patients) is accurate and up to date
- Inform the Trust of any changes to personal data they have provided, e.g. change of address, change of name, photographic identity
- Check the accuracy of data, including sensitive data, which the Trust may send out from time to time, in order to update existing personal data.
- Understand that they must be appropriately trained and supervised to handle Data including requests for the disclosure or sharing of Data

3.4 Employees have the right to request a copy of their personal data held by the Trust (see Section 18 – Written Requests to Supply Data).

3.5 Any breach of this Policy and Procedure may result in disciplinary action being taken.

Possible Consequences of a Breach of Confidentiality (From the Trust Code of Conduct for Staff)

The Trust employs three levels of breach relating to confidentiality. Penalties for these infractions will range from informal warnings through to dismissal.

- Minor Misconduct: Inadvertent disclosure of privileged or confidential information.
- Serious Misconduct: Careless disclosure of privileged or confidential information.

- Gross Misconduct: Deliberate disclosure of privileged or confidential information to unauthorised people.

3.6 Head of Information

For the purpose of implementation of this Policy, the Head of Information is the nominated Data Protection Lead for the Trust and is responsible for reviewing the Data Protection Register annually and for notifying the Information Commissioner of any changes within 28 days.

The Head of Information, in conjunction with the Director of Human Resources, will determine, through appropriate management and the use of strict criteria and controls, the purpose for which non-clinical personal data can be processed.

3.7 The Caldicott Guardian

The Caldicott Guardian has lead responsibility for strategy and governance issues (relating to patient information), confidentiality & data protection expertise, internal information processing and information sharing with external bodies.

The Caldicott Guardian will authorise the sharing of patient information when consent has not been obtained.

3.8 Health Records Manager

The Health Records Department will ensure health records are maintained according to national legislation and guidance. The Health Records Manager will act as the Data Officer in relation to clinical data/health records.

As designated by the Health Records Manager, Health Records representatives will collect and process appropriate data and only to the extent that it is required to fulfil operational needs or to comply with any statutory or information governance standards.

The Health Records Department will provide practical support and advice to all employees on the application of this Policy in relation to clinical data/health records.

3.9 Director of Human Resources

The Human Resources Department must ensure that personal data held by them is protected from unauthorised or unlawful access, loss or disclosure. The Director of Human Resources will act as the Data Officer in relation to HR records.

As designated by the Director of Human Resources, Human Resources representatives will collect and process appropriate data and only to the extent that it is required to fulfil operational needs or to comply with any statutory or information governance standards.

The Human Resources Department will provide practical support and advice to all employees on the application of this Policy in relation to non-clinical data.

3.10 Director of Estates and Facilities

Shall be responsible for compliance with the DPA and related legislation in relation to personal data obtained through the Directorate's activities including:

- Telephone logging
- The use of CCTV

3.10 Trade Unions/Employee Representatives

Trade unions will collect and maintain personal data in order to provide membership services and comply with certain statutory obligations.

All personal data will be treated with the utmost confidentiality and with appropriate levels of security.

3.11 Contractors/Consultants/Partners or other Servants or Agents

All collaborators with the Trust must ensure that:-

- They and all of their employees who have access to personal data held or processed for or on behalf of the Trust are aware of this Policy and are fully trained in and are aware of their duties and responsibilities under the DPA. Any breach of any provision of the DPA will be deemed as being a breach of any contract between the Trust and that individual, company, partner or firm.
- Data Protection audits required by the Trust are permitted upon request
- The Trust is indemnified against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

4. DEFINITIONS

DPA	The Data Protection Act 1998
ICO	The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Data	Information held on a computer, filing system or part of any accessible record
Personal Data	Information relating to a living individual who can be identified from the Data and other information in the possession of the Data Controller and includes any expression of opinion about that individual.

Data Controller	The Rotherham NHS Foundation Trust
Data Protection Lead	A person who either alone or jointly in common with others determines the purposes for which personal data will be used.
Data Officer	A person designated by the Data Controller to process data requests and jointly ensure methods are in place to secure personal data. The Director of Human Resources & Health Records Manager will carry out this role within the Trust.
Data Subject	An individual who is the subject of the personal data being kept
EEA	The European Economic Area
JC & NC	Management and Staff side joint committee
HMB	Hospital Management Board
IGSG	Information Governance Steering Group

5. EQUALITY IMPACT ASSESSMENT

5.1 The Trust aims to design and implement services, policies and measures that meet the diverse needs of its service, population and workforce, ensuring that none are placed at a disadvantage. See **Appendix 3** for the results of the assessment on this policy.

6. CONSULTATION AND RATIFICATION PROCESS

6.1 The Head of Information (on behalf of the Information Governance Steering Group - IGSG) will lead on and develop this Policy in conjunction with the Human Resources Director and Health Records Manager.

6.2 As this Policy impacts on all staff, the Joint Consultative and Negotiating Committee and the Medical Staff Policy Group will be consulted on major changes to the policy.

6.3 The IGSG will lead on this policy and approve minor changes

6.4 Final approval will be required from the Health Informatics Steering Committee, or on major changes to the policy.

7. REVIEW AND REVISION ARRANGEMENTS

7.1 This Policy will be reviewed by the IGSG within the timescales detailed on the contents page.

7.2 The Head of Information will be the lead officer for ensuring the policy is reviewed and approved according to the method identified.

7.3 Major changes required due to legislative requirements or in the light of experience or new found knowledge will require consultation prior to approval by the Health Informatics Steering Committee. Minor changes will be agreed by the IGSG.

8. RELATED DOCUMENTS AND REFERENCES

Acceptable Use & Security IT Policy for Users
Health Records Policy
Information Governance Policy
Policy on the Use & Protection of Patient Information (Confidentiality Code of Conduct)
Records Management Policy
Risk Management Policy
Safe Haven Policy

The Data Protection Act 1998
Freedom of Information Act 2000
NHS Information Governance Toolkit
Data Protection Good Practice – Information Commissioners Office
NHS Employers – Policies and best practice procedures
Benchmarking other NHS and Public Sector Data Protection practices

9. MONITORING OF POLICY COMPLIANCE

Internal audits of the application of this Policy will be carried out on an annual basis and relevant action delegated accordingly.

Health Records will undertake audits of processes related to subject access requests for health records, and the Human Resources Department will undertake audits of processes related to subject access requests for non-health records.

Overall monitoring of the Policy will be actioned by the Information Governance Steering Group.

10. DISSEMINATION AND IMPLEMENTATION

The Data Protection Policy and Procedure will be published on the Information Governance section of the Intranet and emailed to all Heads of Departments. Line Managers will be required to notify employees of its existence at departmental team briefs and attend appropriate training events where necessary.

11. REGISTRATION AND NOTIFICATION TO THE INFORMATION COMMISSION

The Head of Information is responsible for notifying the Information Commission regarding its Register Entry and for supplying details of any subsequent amendments.

The Register Entry describes in general terms, the personal data being processed by the Trust and includes:

- Staff Administration
- Accounts and Records
- Health Administration and Services
- Research
- Crime Prevention and Prosecution of Offenders
- Public Health
- Administration of Membership Records

12. THE EIGHT PRINCIPLES OF DATA PROTECTION

12.1 The Data Protection Act stipulates that anyone processing personal data must comply with the **Eight Principles** of good practice. These Principles, which are legally enforceable, are as follows:-

- Data must be processed fairly and lawfully
- Data must only be used for specified purposes
- Data must be adequate, relevant and not excessive
- Data must be accurate and up to date
- Data must not be kept for longer than necessary
- Data must only be processed in accordance with the rights of Data Subjects
- Data must be held securely
- Data must not be transferred outside the European Economic Area without adequate protection

13. RIGHTS OF THE DATA SUBJECT

- To access information of which they are the subject
- To consent or to withhold consent
- To opt out of direct marketing
- To restrict automated decision making
- To ask for an assessment
- To apply for subject access

14. EXEMPTIONS

The rights of Data Subjects can be restricted on the following grounds:-

- National security
- Crime and taxation

- Health, education and social work
- Regulatory activities
- Journalism, literature and art
- Research, History and statistics
- Legal privilege
- Confidential references given by the Data Controller
- Further categories introduced by the Secretary of State

15. SENSITIVE PERSONAL DATA

The DPA makes a distinction between personal data and “sensitive” personal data which refers to the following:-

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade Union membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions

Sensitive personal data can be processed provided that at least one of the following conditions have been met:-

- The Data Subject has given their **explicit consent**
- It is necessary for monitoring equal opportunities
- It is a legal requirement of the subject’s employment
- It is necessary to protect the vital interests of the subject
- It is carried out by certain non-profit bodies established for political, philosophical, religious or trade union purposes
- It is necessary for legal proceedings
- It is necessary for medical purposes
- The Secretary of State has given consent
- It is necessary for the prevention or detection of any unlawful act
- It is necessary for the provision of services such as confidential counselling or advice
- It is necessary for insurance or occupational pension scheme contracts

This list is not exhaustive and new categories may be added by the Secretary of State.

16. PROCESSING DATA

An essential requirement of the DPA is that all data must be processed “fairly”. The Trust will therefore ensure that:-

- The Data Subject will not be deceived or misled
- The Data Subject will be informed of the purpose for which the personal data is intended to be used by the Information Officer or their nominated deputy

- The Data Subject will be informed whether the data is likely to be passed to a third party

17. TRANSFERRING DATA ABROAD

17.1 Personal Data will not be transferred outside of the United Kingdom unless that country or territory "ensures adequate level of protection" for the rights and freedoms of Data Subjects.

17.2 Transfers of Data may take place:

- Where the data subject has given **explicit consent**
- It is necessary to perform or make a contract
- By reason of substantial public interest
- Is part of Personal Data on a Public Register
- Is on terms approved by the Information Commissioner

18. WRITTEN REQUESTS TO SUPPLY DATA

18.1 The Trust maintains two processes for Data Subjects to request records. These are outlined in **Appendix 1** (Release of Health Records) and **Appendix 2** (Release of Non-Health Records).

18.2 Upon written request from the Data Subject, the Data Officer, or their nominated deputy, is obliged to supply:-

- A description of the Data
- The purpose for which Data is being held
- The source of the Data
- The person(s) to whom the Data will be or may be disclosed

18.2 A maximum **charge of £10.00 for non-health records and £50.00 for health records** will be payable by the Data Subject to the Trust for the supply of Data.

18.3 Proof of identity will be required to ensure that data is provided to the correct individual. Where a request is made in person, two original pieces of documentation, for example a recent utility bill or bank statement showing the individual's name and current address, will be required. In some cases additional details such as a passport or photo ID driving licence may be required due to the sensitive nature of the information held. Where the request is to be sent via the post, this will only be sent to the registered address for the individual. If another address is stipulated, this will be investigated further to determine the legitimacy of the request.

18.4 The Data Officer will supply everything held at the time the application was made within **40 working days** (see section 19.1 below regarding disproportionate effort).

19. WITHHOLDING DATA

19.1 Data maybe withheld either if the Subject agrees or the supply of information would involve disproportionate effort.

19.2 Data may also be withheld if it identifies a third party.

20. OPTING IN/OUT

20.1 Employees must read carefully any documentation which implies their consent to the processing of personal data, for example, the completion of a booking form for a conference which states that information may be used for other specific purposes.

20.2 On occasions where an employee may be asked to participate in any photographic or other publicity campaign on behalf of the Trust, consent will be assumed at the time unless the employee explicitly opts out.

20.3 Employees have the right to opt out of Direct Marketing and in deciding to do so should ensure that the relevant tick box is completed to withdraw personal details from any database.

20.4 The Trust will ensure that employees are kept informed of the methods used to arrive at any automated decisions (e.g. job applications) thereby giving the choice of opting out of the process.

RELEASE OF HEALTH RECORDS

The Trust has a duty to ensure that requests for clinical information in respect of medico-legal matters are dealt with efficiently and speedily.

Implementation of the subject access section of the Data Protection Act/Access to Health Records Act is the overall responsibility of the Health Records Manager throughout the Trust, and processed through the Administration Office in the Health Records Department.

Apart from the patient, requests for access to patient records can be received from various sources which could include solicitors, the police, the Department of Social Security, the Criminal Injuries Compensation Board, the War Pensions Department, Insurance Companies and Consultants outside the Trust. The Trust has a response mechanism to deal with requests for access in respect of records from whichever source stated above. However, to support these clearly defined procedures the following general principles should be adhered to:-

Outside Agency Access

- On receipt of a written request, the Administration Team will ensure that this is dealt with promptly.

- Always be aware of the need for confidentiality.

- Never send original records or original material of any kind.

- A charge will be made for copying. The charge is governed by a maximum fee of £50.00 as stipulated in the Data Protection Act 1998.

- **All** staff should always consult with the health records manager before releasing patient records.

- The police do not have the right of access to a patient's healthcare records. However they may have photocopies with patient consent or with presentation of a Court Order, which must be placed on file. There may, at times, be exceptions to this, therefore advice should be sought from the Caldicott Guardian (or designated deputy) if there are any concerns about disclosure.

- Solicitors acting on behalf of a patient must provide their client's signed authorisation before disclosure of copy records is undertaken.

- Anyone seeking a patient's record by use of an Enduring Power of Attorney must provide a Registered Certificate which must be placed on file.

- Anyone, other than next of kin, seeking a deceased patient's records must produce Probate or Letters of Administration or a Court Order before disclosure is undertaken.

- The Coroner may require access to a patient's original healthcare records and the Trust should assist wherever possible. If in doubt advice may be sought from the patient liaison office.

Patient Access

In respect of the right of access awarded the patient to his/her patient record, the Data Protection Act 1998 is specific. Those with this right include the patient; a person authorised in writing to apply on behalf of the patient; the person having parental responsibility for the patient; a person appointed by the Court to manage the affairs of a patient who is deemed incapable (e.g. power of attorney) and, where a patient has died, his/her personal representative, or any other person having a claim arising from the death.

- Patients have a right of access to their records without charge provided the request is made within 40 days of the record being made.

- The Act only applies to notes made in the patient's record after the 1st November 1991.

- The Administration Team will generate a proforma and leaflet (see below), - 'Request for Access to Health Records' – which **all** applicants must complete when requesting access.

- A fee will be charged for photocopying and postage.

- If the patient considers the records to be inaccurate, they can be corrected. But only after discussion with the relevant health professional, if it is agreed that the record is inaccurate.

- Under certain circumstances access may be refused.

These circumstances can be as follows:-

- Where, in the opinion of the holder of the record, giving access would disclose information likely to cause serious harm to the physical or mental health of the patient or any other individual.

- Where giving access would, in the opinion of the holder of the record, disclose information relating to or provided by an individual other than the patient who could be identified from that information.

- Where the relevant part of the clinical record was made before the 1st November 1991. (However, access to these records is generally allowed).

Charges and Fees

The Trust operates a sliding scale of charges for reproducing healthcare records and X-rays. The charges are governed by the maximum fee (currently £50.00) stipulated in the Data Protection Act 1998.

Complete guidance on the current status of the Data Protection Act 1998/Access to Health Records Act 1990, issued by the NHS Management Executive, can be obtained from the Health Records Manager.

APPLICATION FORM

Request No: ☐

ROTHERHAM GENERAL HOSPITAL NHS FOUNDATION TRUST

Request for Access to Health Records
(under the Data Protection Act 1998)

Please read the accompanying notes before filling in this form

PART A: IDENTITY OF PERSON ABOUT WHOM INFORMATION IS REQUESTED (SEE NOTE 1)

SURNAME		**(FORMERLY)**	
FORENAME(S)		**DATE OF BIRTH**	
CURRENT ADDRESS		**PREVIOUS ADDRESS** **GP**	
TEL. No:			

Approximate date of change of address

PART B: DETAILS OF RECORDS TO BE ACCESSED (SEE NOTE 2)

CONSULTANT/ DEPARTMENT	CONDITION OR ILLNESS	APPROXIMATE DATE

PLEASE SPECIFY REASON FOR THIS REQUEST

PART C: DECLARATION (SEE NOTE 3)
(to be signed in the presence of the person confirming identity)
I declare that the information given in this form is correct to the best of my knowledge and that:
(tick one box only)

☐ **I am the patient named in Part A**
(Complete Part A, B, C and D)

☐ **I have been authorised to act by the patient**
(Complete Part A, B, C, D and E)

☐ **I am the patient's representative. The patient is incapable of understanding the request (*by virtue of age, is severely mentally ill, is severely mentally handicapped)**
(Complete Part A, B, C, D and E)

☐ **I am the deceased patient's personal representative and attach confirmation of my appointment**
(Complete Part A, B, C, D and E)

☐ **I have a claim arising from the patient's death and wish to access information relevant to my claim and attach details of the grounds of my claim**
(Complete Part A, B, C, D and E)

PART C: DECLARATION (Continued)

SIGNED		**DATE**	
ADDRESS IF DIFFERENT FROM THAT AT PART A OVERLEAF (if applicable)			
TELEPHONE NO. (if applicable)			
RELATIONSHIP TO PATIENT (if applicable)			

PART D: CERTIFICATION OF APPLICANT (SEE NOTE 4)

I _____ certify that I have known _____
for _____ years and certify that I have just witnessed this person sign this Request for Personal Information under the Data Protection Act 1998.

SIGNED		DATE	
ADDRESS :			
DAYTIME TELEPHONE NO FOR CONFIRMATION OF IDENTIFICATION			

PART E: AUTHORISATION WHERE APPLICANT IS NOT THE PATIENT (SEE NOTE 5)

I hereby authorise release of my health records, as specified above, to the person named in Part C above, and declare that I am the patient named in Part A of this form.

SIGNED		**DATE**	

WARNING

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.

PAYMENT: (SEE NOTE 6)

PLEASE RETURN THIS FORM TO:

Deputy Health Records Manager
Rotherham General Hospitals NHS Trust
Moorgate Road
Rotherham
S60 2UD

NOTES FOR APPLICANTS

ROTHERHAM GENERAL HOSPITAL NHS FOUNDATION TRUST

Request for Access to Personal Information

(under the Data Protection Act 1998)

Please read these notes before completing the application form

Accompanying Notes

Please complete the application form in block capitals (other than signature) and black ink

Note 1 (Part A)

This part must be completed for all applications

Please complete all details relating to the patient whose record you wish to access. This should include former names (e.g. maiden name) and a previous address, if applicable, for the period relating to the record requested. The name of your GP should be given. Hospital number should be stated, if known.

Note 2 (Part B)

This part must be completed for all applications

You must specify the reason why and which records you are requesting access to and provide as many details as possible. It is not sufficient merely to state 'All Records'. If you have insufficient space, please attach a continuation sheet containing full details. Examples are given below:

Consultant/Dept	Condition or Illness	Approximate Date
Mr Jones	Appendicitis	December 1991
Physiotherapy	Broken Leg	January 1992

Note 3 (Part C)

This part must be completed for all applications

Part C tells us who you are and must be completed in the presence of a witness, who must also complete Part D.

Tick one box only which best describes you

Please sign and date in the space provided, and if you are not the patient, provide your address, telephone number and relationship to the patient.

Note 4 (Part D)

This part must be completed for all applications

The person who witnessed the completion of Part C must complete this section. They should insert their full name, the applicant's name and the period that they have known the applicant in the spaces provided.

They should then sign and date, as indicated, and provide their own address and daytime telephone number.

Note 5 (Part E)

This part should only be completed when the applicant is not the patient but has been authorised by the patient to make the application. The patient should sign and date in the space provided, to officially authorise the applicant's request for access.

Note 6 (Payment)

If the records you are requesting were made more than 40 days prior to the date of this application, then an administration fee of £10 will be charged along with photocopying and postage fee. You will be notified of the total cost when your notes are ready for release. Copies will be sent on receipt of a cheque or Postal Order which should be made to Rotherham General Hospitals NHS Trust.

General Notes

1. **WARNING** – You are advised that the making of false or misleading statements in order to obtain access to Personal information to which you are not entitled is a criminal offence.

2. Patients have a right to confidentiality of their personal health information and the hospital must be satisfied that an applicant is the patient or the patient's authorised representative. This may involve checking the identity of any of the (named) persons on the application form, and we may also have to make further enquires. Where possible telephone confirmation will be sought. However, it may be necessary to request further proof of identity, e.g. driving licence.

3. Receipt of your application will not be acknowledged, but will be dealt with within the time limits specified in the Data Protection Act 1998, i.e. 21 or 40 days dependent upon the age of the record.

4. Information may be withheld where it is considered that access might cause serious harm to the physical or mental health of the patient or any other individual, or where a third party might be identified. There is no requirement to disclose the fact that information has been withheld.

The Rotherham NHS
NHS Foundation Trust

Can I see my Health Records?

Your questions answered

The Rotherham NHS Foundation Trust

Q *Have I the right to see my health records?*

A Yes. Under the Data Protection Act 1998 you have the right to see health records. You can ask to see a particular part of the record or all of it. However it may be more helpful to specify the part of the record you are interested in.

Q *What records can I see?*

A For records concerning your hospital care the act covers information about your physical or mental health recorded by any doctor, nurse, midwife or any other health professional.

Q *Can any of my health records be withheld from me?*

A Yes. Any health professional can refuse to disclose information which they consider is likely to cause you or anyone close to you serious physical or mental harm. The professional is not obliged to tell you that they are with holding information. Therefore you may wish to ask whether you have been given all the information you need.

Q *How can I get to see my records?*

A You should first ask to see the record holder, that is usually the doctor or nurse, to see what they have written in the records. You can do this at any time during your stay in hospital or at any out-patient appointment. If there is any problem you should ask for an application form. See the contact person and telephone number at the end of this leaflet.

Q *What happens if I cannot understand the record?*

A The record holder must explain any part of the record which you cannot understand.

Q *What should I do if something is wrong with my records?*

A If you believe that any facts in the record are wrong, you can ask the record holder to change them. The record holder must either correct the record or note your disagreement. If you think you have had your right to access unfairly denied you can complain. You can do this through the hospital complaints procedure. Your local Community Health Council will give you advice.

Q *Will I be able to have a copy of my records?*

A Yes. Copies can be made, but you will have to pay a fee depending on what you require. It will be helpful if you specify which part of the record you want copied. You will be invoiced for the amount once your records have been sent out to you.

Q *How long will it take for my records to be made available to me?*

A Within 21 days if your application relates to an entry made in your records within the past 40 days, or 40 days if there has been no recent entry.

Confidentiality

Patients have the right to confidentiality of their personal health information and the Trust must be satisfied that an applicant is the patient or their authorised representative.

How to Apply

Application forms can be obtained by either writing to:

Assistant Medical Records Manager
Rotherham General Hospital
Moorgate Road
Rotherham
S60 2UD

Or by Telephoning:

01709 304254

Further information and advice is available from:

Rotherham Health Advice Centre
Bridgegate
Rotherham

Subject Access Request Form
Non-Health Records

THE DATA PROTECTION ACT 1998

SUBJECT ACCESS REQUEST FORM – NON HEALTH RECORDS

Please refer to the attached guidance notes overleaf.

SECTION A : PERSONAL DETAILS

Surname:	Former name (if applicable):
MR/MRS/MISS/MS:	First Name(s):
Date of Birth:	Employee No:
Present Address:	Post Code Telephone No: Mobile No:

SECTION B: DETAILS OF THE DATA REQUESTED

Subject/Topic/Area

SECTION C: PROOF OF IDENTIFICATION

Documents Supplied (See attached Guidance Notes)

SECTION 4: PAYMENT

Please enclose a cheque for £…….. made payable to The Rotherham NHS Foundation Trust

The completed form, fee and supporting proof of identity should be submitted to:
Graham Briggs, Data Officer, Rotherham General Hospital, Moorgate Road, Rotherham S60 2UD

Signature of applicant: …….. Date ……

PRINT NAME: ……

SUBJECT ACCESS REQUEST FORM GUIDANCE NOTES – NON HEALTH RECORDS

1. **Personal Details**: Please complete your personal details as requested. Please tell us if you have been previously known by any other name. If you are requesting historical information, please provide as many details as possible, e.g. previous addresses (use a separate sheet if necessary.

2. **Details of the Data you require**: You should give as much assistance as you can about particular areas to search so that we can give you what you require without delay. You should also give any relevant reference numbers that might be useful. These details are required to assist in locating the data so that you can be given a copy of everything.

3. **Proof of Identification**: Proof of name and address is required to ensure we only give information to the correct person. We require two original pieces of documentation, for example, a recent utility bill, bank statement (photocopies are not acceptable) showing your name and address. In some cases, additional details such as a passport or photo ID driving licence may be required due to the sensitive nature of the information held.

4. **Keep your documents secure**: Always send important documents by recorded delivery or other special post as necessary. The Trust can not be held liable for items lost in the post.

5. **Payment**: A search fee of (maximum) £10.00 is required for each separate request. The fee is not refundable if the result of the search shows that there is no data to be found.

   Please make your cheque payable to: The Rotherham NHS Foundation Trust

6. **If you have any questions** relating to identification requirements or any other aspect of a subject access request, please contact the Director of Human Resources by email on Graham.Briggs@rothgen.nhs.uk or telephone the Human Resources Department on 01709 304508.

Service/Clinical/Non Clinical Area assessed	**Title of plan, policy and/or procedure being assessed**	**Date of Assessment**
Trust Wide	Data Protection Policy	08 JAN 09
Manager conducting assessment, including contact details	Scott Reid, Head of Information ext 4195	

Reason for assessment:

To ensure that the Data Protection Policy meets the General Duty to promote Race, Disability and Gender Equality.

Outcomes and Results of the Initial Assessment:

Current processes do not regularly provide application forms in languages other than English, or in brail. There is no record of this being required, and if needed, other mechanisms could be utilised to enable a translation or assistance. It is recommended that the application form be amended to highlight this, and agree a process.

Signed off by lead officer(s)- name and date required: Scott Reid – 08/01/09

Please complete EIA Next Steps Template(Please refer to page 37-38 of this EIA Toolkit) and send page 38 to Head of Equality and Diversity