Trust Policy

Worcestershire Acute Hospitals NHS Trust

Subject Access Request Policy

Department / Service:	Corporate
Author/Owner:	Jane Clavey, Head of Legal Services
Accountable Director:	Kimara Sharpe, Company Secretary
Approved by:	Trust Leadership Group
Date of approval:	18th April 2018
Revision Due:	April 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:

This policy sets out the processes that are in place to deal with Subject Access Requests under the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Access to Health Records Act (1990)

Latest Amendments to this policy:

Revised in line with GDPR, effective from 25.05.2018
Revised forms for GDPR and ATHR applications

Contents page:

1. Introduction

A Subject Access Request is a request from a person asking an organisation to provide them with information relating to that person which is held or processed by the organisation.

The disclosure request may be direct (e.g. individual request for a copy of their health records) or may form part of an investigation (e.g. a request for a statement by the Police). The request may be vague or imprecise and may be relevant to a claim against the organisation. The person requesting the data does not need to give a reason for wanting access however they only have a right to see information about the data subject, they have no right to see information which is not personal data at all or is only about third parties.

1.1 General Data Protection Regulations (GDPR)

Individuals have several rights in relation to the information held about them. Access gives them the right to obtain a record in permanent form.

The GDPR states that individuals [Identifiable Natural Person – GDPR art4(1)] have a right to obtain confirmation as to whether or not personal data concerning them is being processed, and where that is the case to have access to that personal data. The Individual can access the data held about them by make a request in writing for a copy of the information the Trust holds about them, both in electronic format and in paper.

1.2 Access to Health Records Act 1990 (ATHR)

This Act has been repealed to the extent that it only relates to the health records of deceased patients. It applies only to records created since 1st November 1991. Applications for disclosure of records for deceased patients should only be granted to the personal representative of the estate or to someone having a claim arising out of the death.

1.3 Freedom of Information Act 2000

Applications for information of a personal nature cannot be made under the Freedom of Information Act 2000.

2. Scope of this document

This policy deals with the rights of Data Subjects whereby individuals can request access to their personal data.

This policy applies to all requests for access to personal data held by the Trust. This applies to anyone about whom the Trust holds information – including staff, ex-staff, patients and other service users.

This policy provides a framework for the Trust to ensure compliance with the GDPR 2016 and Access to Health Records Act 1990. This policy is supported by operational procedures and activities as detailed in appendices 1-3.

3. Definitions

Data	The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudo-anonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
Personal Identifiable Information (PII)	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
Sensitive Personal data	The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data where processed to uniquely identify an individual, data concerning health or data covering and individual's sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
Identifiable Natural Person (INP)	The person the information is about and who can be identified from that information. All Identifiable Natural Persons have certain legal rights in relation to their personal identifiable information.
Health Record	A 'health record' is defined as being any record which consists of information relating to the physical or mental or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual. The definition can also apply to material held on an x-ray or an MRI scan. This means that when a subject access request is made, the information contained in such material must be supplied to the applicant.
Employment Record	An 'employment record' is defined as being any record which consists of information relating to a current or former member of staff and has been made by or on behalf of the Trust in connection with the individual's employment.
Occupational Health Record	An 'occupational health record' is defined as being any record which consists of information relating to the physical or mental or condition of a current or former member of staff and has been made in connection with the individual's employment.
Complaint File	A 'complaint file' is defined as being any record which consists of information relating to a complaint made by a patient or a representative acting on their behalf.
Incident File	An 'incident file' is defined as being any record which consists of information relating to an incident involving a patient; employee; contractor or visitor.

4. Responsibility and Duties

The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information, making sure it is used properly and enabling appropriate information-sharing.

The Data Protection Officer is responsible for providing advice and guidance about GDPR to work colleagues at all levels.

The Head of Legal Services has responsibility for ensuring all Subject Access Requests regarding health records are actioned.

The Complaints Manager has responsibility for ensuring all Subject Access Requests regarding complaints are actioned.

The Patient Safety and Risk Manager has responsibility for ensuring all Subject Access Requests regarding patient safety incidents and alerts are actioned.

The Head of Human Resources is responsible for requests by employees or ex-employees for copies of their personal employment files (this includes both medical and non-medical staff)

All managers must ensure their staff are aware of this policy and procedure and know how to deal with requests for personal/patient identifiable information.

5. Who can make an application for personal data?

- The Data Subject
- A person lawfully acting on their behalf:
  - Their lawyer with consent form
  - Person with parental responsibility for under 13s [GDPR c2 art8]
  - Person with authority to manage affairs of an incapacitated adult [Refer to Mental Capacity Act]

Where the patient is deceased, the relevant authority must be provided.

6. Timescales

It is important that action is taken promptly as the legislation dictates that the information must be provided without delay and at the latest within one month of receipt of the request.

The timescale for the period of compliance may be extended by a further two months where requests are complex or numerous. If this is the case, the individual must be informed within one month of the receipt of the request and an explanation given as to why the extension is necessary.

7. Charges

A copy of the information must be provided free of charge. However, when a request is manifestly unfounded or excessive, particularly if it is repetitive a ‘reasonable fee’ can be charged.

A reasonable fee can be charged to comply with requests for further copies of the same information. This does not mean a charge can be applied to subsequent access requests.

The fee must be based on the administrative cost of providing the information.

8. Provision of the Information Requested

The identity of the person making the request must be verified using ‘reasonable means’.

If the request is made electronically, where possible the information should be provided in a commonly used electronic format.

8.1 Requests for large amounts of personal data
Where a large quantity of information is processed about an individual, the GDPR permits the Trust to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not include an exemption for requests that relate to large amounts of data, but the Trust may be able to consider whether the request is manifestly unfounded or excessive (see 8.3 below).

8.2 The Duty to Search
Searches need to be reasonable and proportionate. Disproportionate effort is not restricted to supply of copies but includes difficulties which occur in the process of complying with the request which may result in supply. The threshold of proportionality is high. The person dealing with the request must be able to provide evidence to show what has been done to identify personal data and the relevant plan of action. Deleted data may need to be provided depending on how difficult it is to recover. Deciding it is all too difficult will not amount to compliance.

8.3 Manifestly unfounded or excessive requests
Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Trust can:

- Charge a reasonable fee taking into account the administrative costs of providing the information; or
- Refuse to respond.

Where the decision is made to refuse to respond to a request, an explanation of the reason must be given to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. The individual should be informed of the decision without undue delay and at the latest within one month of receipt of the request.

Advice should be sought from the Data Protection Officer.

9. Rectification

Article 5(d) of the GDPR requires that personal data shall be “accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal date that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”.

9.1 When should personal data be rectified?
Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If the personal data in question has been disclosed to others, each recipient must be contacted and inform of the rectification - unless this proves impossible or involves disproportionate effort. If asked, the individual must be informed about these recipients.

9.2 Timescale to comply with a request for rectification
A response to a request for rectification must be complied with within one month of receipt of the request. This can be extended by two months where the request for rectification is complex.

If a decision is taken not to take action in response to a request for rectification, an explanation as to why must be given to the individual, informing them of their right to complain to the Information Commissioner and to a judicial remedy.

Advice should be sought from the Data Protection Officer.

10. Subject Access Requests Process

See appendix 1 Subject Access Requests Flowchart
See appendix 2 Template Subject Access Request Form (GDPR)
See appendix 3 Template Access to Health Records Form – deceased patients

Requests will be monitored through reporting to the Information Governance Steering Group (IGSG)

11. Implementation

11.1 Plan for implementation

The Data Protection Officer will raise awareness of the policy in relevant training sessions and meetings.

The Head of Legal Services; Complaints Manager; Patient Safety and Risk Manager and Head of Human Resources will ensure that requests for access to records for which they are responsible are logged and processed to meet the required timescales for completion.

Staff involved with requests must be trained and be aware of the process to ensure they respond to meet the requirements and timescales detailed in the policy.

11.2 Dissemination

This policy will be published on the Trust's Intranet. It is the responsibility of line managers to ensure that members of staff are made aware of this policy. New members of staff are advised during their induction process to look at the Trusts Internet and Intranet to ensure that they read and have a good working knowledge of all relevant policies, strategies, procedures and guidelines.

11.3 Training and awareness

Annual Data Awareness training is mandatory for all staff. Any staff responsible for handling Subject Access requests must be aware of their responsibilities in complying with the General Data and Security Principles.

Departmental training is given to Legal Services staff responsible for actioning subject access requests for Health Records

12. Monitoring and compliance

This policy will be monitored through summary updates to the Information Governance Steering Group (IGSG) from the Data Protection Officer and the Head of Legal Services. Where requests are not managed within the agreed timescales and standard, the steering group will request actions and monitor the improvement.

Page/ Section of Key Document	Key control	Checks to be carried out to confirm compliance with the Policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Section 5	Requests will be monitored through reporting to IGSG	Reports to IGSG	Twice yearly	Company Secretary	IGSG	Twice yearly

13. Policy Review

The Information Governance Steering Group will review this strategy on a bi-annual basis. Where national policy or legislation dictates change, review will be carried out at an earlier point if appropriate.

14. References:

References:	Code:
Information Commissioner's Office – Guide to the General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Access to Health Records Act 1990	www.opsi.gov.uk/acts/acts1990
Freedom of Information Act 2000	www.opsi.gov.uk/acts/acts2000
Trust Information Governance Policy	WAHT-CG-579

15. Background

15.1 Equality requirements

None – equality assessment: Supporting Document 1

15.2 Financial risk assessment

Yes – financial risk assessment: Supporting Document 2

15.3 Consultation

The Policy has been updated by the Head of Legal Services with input from the Data Protection Officer; Complaints Manager; Patient Safety and Risk Manager and Head of Human Resources.

Contribution List

This key document has been circulated to the following individuals for consultation:

Designation
Assistant Director of Information and Performance
Assistant Legal Services Manager
Business Change and Records Lead
Company Secretary / Data Protection Officer
Deputy Director of Nursing
Director of Asset Management and ICT
Director of Finance / SIRO
Head of Human Resources
Head of Legal Services
Head of Systems and Development
Information Governance Manager
Information Governance Officer
Legal Services Assistant
Patient Safety Lead - Caldicott Guardian
Service Delivery Manager – ICT

This key document has been circulated to the chair(s) of the following committee's / groups for comments:

Committee
GDPR Working Group
Information Governance Steering Group
Trust Leadership Group

15.4 Approval Process

This strategy will be approved by the Trust Leadership Group bi-annually.

15.5 Version Control

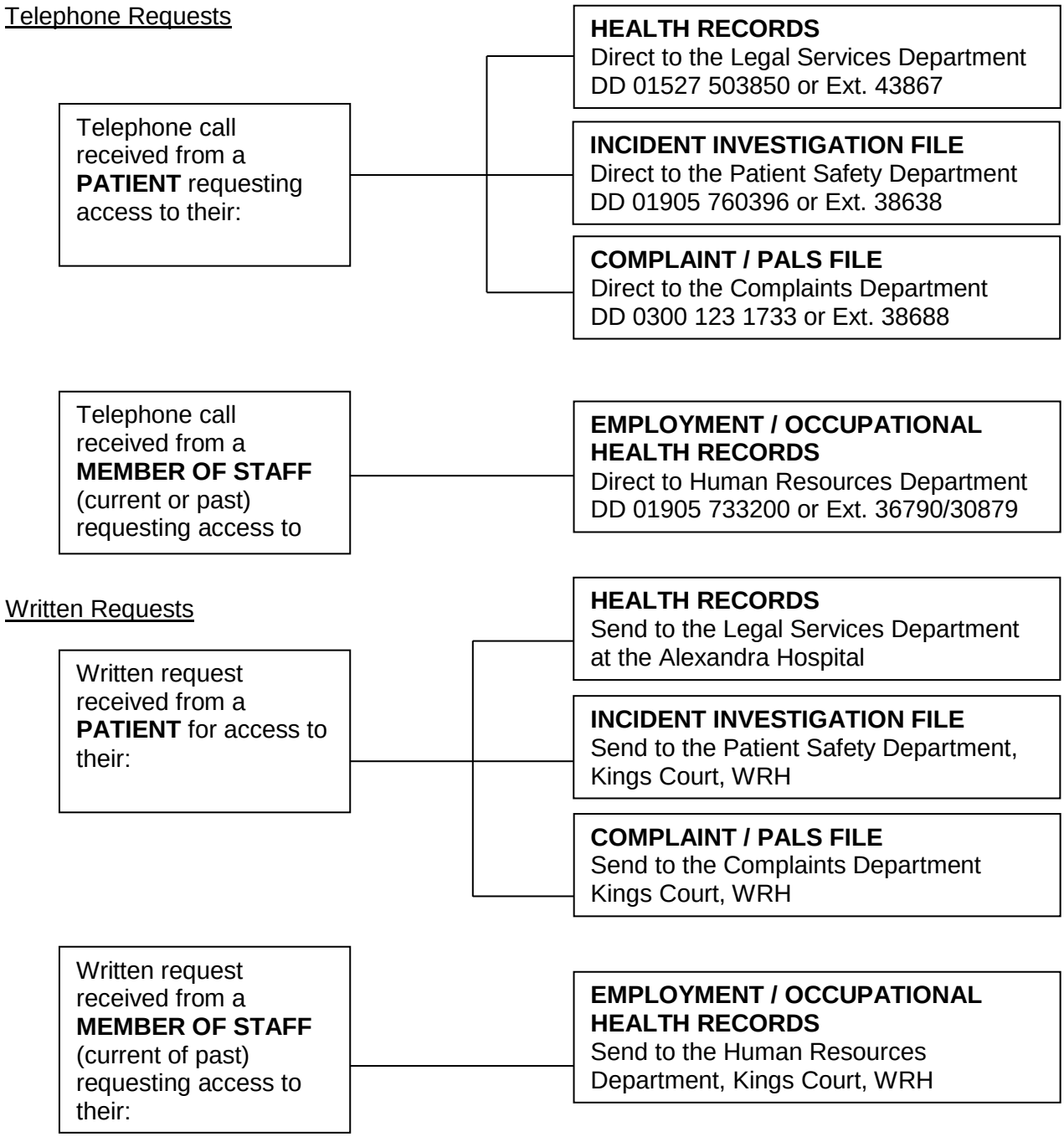
This section should contain a list of key amendments made to this document each time it is reviewed

Date	Amendment	By:
April 2018	Updated to reflect implementation of GDPR	Head of Legal Services
May 2017	Title change of Patient Services to Complaints, PALS and Bereavement Services	Head of Legal Services
May 2015	Updated into the most recent Trust Policy format Updated SAR health Records Guidance and Application included Reporting structure and other minor amendments included	IG Manager
Feb 2013	Policy created	IG Manager

Appendix 1
Subject Access Requests Flowchart

Worcestershire Acute Hospitals NHS Trust

Dealing with Subject Access Requests – if not sent directly to the correct department



All other telephone calls or written requests regarding subject access requests that do not fit within any of the categories above should be directed to the Data Protection Officer.
Direct dial 01905 733962 or Ext. 30716 or send to the Executive Office, Sky Level, WRH

Appendix 2
Template Subject Access Request Form (GDPR)

NHS Worcestershire Acute Hospitals NHS Trust

ACCESS TO RECORDS UNDER THE GENERAL DATA PROTECTION REGULATIONS (GDPR) 2016

NOTES FOR APPLICANTS

Please read these guidance notes before completing the Application Form

Note 1 (Part A) – Identity of the person about whom the information is requested
This part must be completed for all applicants.

Complete all details relating to the person whose records you wish to access. This should include former names (e.g. maiden name) and previous address, if applicable, for the period relating to the record requested.

If requesting access to health records please provide the Hospital Registration Number and NHS Number if known.

Note 2 (Part B) – Details of the information required.
This part must be completed for all applicants.

You must specify the records you wish to access and provide as many details as possible. It is not sufficient to state "All Records". If there is insufficient space, please attach a continuation sheet.

Note 3 (Part C) – Declaration
This part must be completed by the person seeking access.

Tick one box only which best describes you.

Sign and date in the space provided, and if you are not the person to who the record relates, provide your address, telephone number and relationship to the person.

You will need to supply a form of identification: either a current photo driver's licence or a current photo passport. If the person lacks capacity of understanding to make the request you also need to provide a copy of the authority enabling you to act on their behalf e.g. Lasting Power of Attorney.

We require proof of identity before we can process your request. This is to protect the identity of the data subject and ensure that the Data Protection principles are not breached. Photocopies are acceptable, DO NOT send original documents.

Note 4 (Part D) – Authorisation for Application made on behalf of another person

This part should only be completed when the applicant is not the person to who the record relates but has been authorised by the person to make the application. *If the application relates to a deceased person's records please contact the Legal Services Department on 01527 503850.*

Once the details in sections A to C have been completed the person should sign and date in the space provided to officially authorise the applicant's request for access.

GENERAL NOTES

1. WARNING – It is a criminal offence to make false or misleading statements in order to obtain information.
2. Individuals have a right to confidentiality of their personal health information and the Trust must be satisfied that an applicant is the person or the person's authorised representative. This may involve checking the identity of any of the named persons on the completed application form and their validity to request access.
3. Information may be withheld where it is considered that access might cause harm to the physical or mental health of the patient or any other individual, or where a third party might be identified.

Appendix 2
Template Subject Access Request Form (GDPR)

Worcestershire Acute Hospitals NHS Trust

PLEASE COMPLETE IN BLOCK CAPITALS

APPLICATION FOR ACCESS TO RECORDS (GDPR)

Part A – Identity of the Person about whom the information is requested (see note 1)

SURNAME:	**FORMERLY:**
FORENAME(S):	**DATE OF BIRTH:**
CURRENT ADDRESS:	**PREVIOUS ADDRESS:**
TEL NO:	
If requesting health records	
HOSPITAL NO:	**NHS NO:**

Part B – Details of the information required (see note 2)

Department	Brief details of information required	Approximate Date(s)

Part C – Declaration (see note 3)

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under the terms of the GDRP. (Tick as appropriate)

☐	I am the person named in Part A
☐	I have been authorised to act by the person
☐	I am the person's parent/legal guardian and have parental responsibility
☐	The person is over 13 years of age. I am their next-of-kin/legal representative. I am making this application as they lack the capacity of understanding to make the request.

SIGNED:	**ADDRESS** (if different from that in Part A)
PRINT NAME:	
DATE:	
TEL NO:	
RELATIONSHIP TO PERSON:	

Appendix 2
Template Subject Access Request Form (GDPR)

Worcestershire Acute Hospitals NHS Trust

Part D – Authorisation for application made on behalf of another person (see note 4)

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

SIGNED:
PRINT NAME:
DATE:

Please confirm the details of the identification information enclosed with the application:

	Photocopy of current photo driver's licence
	Photocopy of current passport
	Authorisation to act on behalf of a person that lacks capacity

WARNING: It is a criminal offence to make false or misleading statements in order to obtain information.

Please return the completed form to …. *INSERT DETAILS ….*

Appendix 3
Template Subject Access Request Form (ATHR)

Worcestershire Acute Hospitals NHS Trust

ACCESS TO RECORDS UNDER THE ACCESS TO HEALTH RECORDS ACT (1990)

NOTES FOR APPLICANTS
Please read these guidance notes before completing the Application Form

Note 1 (Part A) – Identity of the person about whom the information is requested

Complete all details relating to the person whose records you wish to access. This should include former names (e.g. maiden name) and previous address, if applicable, for the period relating to the record requested.

If known, please provide the Hospital Registration Number and NHS Number.

Note 2 (Part B) – Details of the information required.

You must specify the records you wish to access and provide as many details as possible. It is not sufficient to state "All Records". If there is insufficient space, please attach a continuation sheet.

Note 3 (Part C) – Declaration
This part must be completed by the person seeking access.

Sign and date in the space provided provide your address, telephone number and relationship to the person.

You will need to supply a form of identification: either a current photo driver's licence or a current photo passport, and a copy of the authority confirming you are the personal representative of the deceased.

We require proof of identity before we can process your request. This is to protect the identity of the data subject and ensure that the Data Protection principles are not breached. Photocopies are acceptable, DO NOT send original documents.

Charges for processing your application
Requests relating to deceased patient's records are governed by the Access to Health Records Act 1990 allows for a charge to be applied for this service which includes a £10.00 administration fee. Most records are available in an electronic format and will be provided on an encrypted CD. The charge for records in this format is £10.00. Paper records are charged of 30p per page (single sided, A4). If copy radiology (x-rays) is required this information will be provided on an encrypted CD. The charge for x-rays is £10.00. All charges include postage by recorded delivery.

Once the copy information is available you will be notified of the charge. Payment is required before the information is disclosed. Cheques/Postal Orders should be made payable to: WORCESTERSHIRE ACUTE HOSPITALS NHS TRUST
Please note we do not have the facilities to accept payment by credit or debit card.

GENERAL NOTES

WARNING – It is a criminal offence to make false or misleading statements in order to obtain information.

Individuals have a right to confidentiality of their personal health information, even following their death, and the Trust must be satisfied that an applicant is the person's authorised representative. This may involve checking the identity of any of the named persons on the completed application form and their validity to request access.

Information may be withheld where it is considered that access might cause harm to the physical or mental health of the patient or any other individual, or where a third party might be identified.

Please return the completed form to:
Access to Health Records
Legal Services Department
Alexandra Hospital
Woodrow Drive
Redditch
B98 7UB

Appendix 3
Template Subject Access Request Form (ATHR)

Worcestershire Acute Hospitals NHS Trust

PLEASE COMPLETE IN BLOCK CAPITALS

APPLICATION FOR ACCESS TO HEALTH RECORDS (ATHR 1990)

Part A – Identity of the Person about whom the information is requested (see note 1)

SURNAME:	**FORMERLY:**
FORENAME(S):	**DATE OF BIRTH:**
CURRENT ADDRESS:	**PREVIOUS ADDRESS:**
TEL NO:	
If requesting health records	
HOSPITAL NO:	**NHS NO:**

Part B – Details of the information required (see note 2)

Department	Brief details of information required	Approximate Date(s)

Part C – Declaration (see note 3)

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under the terms of the ATHR 1990.

SIGNED:	**ADDRESS** (if different from that in Part A)
PRINT NAME:	
DATE:	
TEL NO:	
RELATIONSHIP TO PERSON:	

Please confirm the details of the identification information enclosed with the application:

	Photocopy of current photo driver's licence
	Photocopy of current passport
	Confirmation the applicant is the personal representative of the deceased

WARNING: It is a criminal offence to make false or misleading statements in order to obtain information.

Supporting Document 1

Supporting Document 1 - Equality Impact Assessment Tool
To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability – learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact Assistant Manager of Human Resources.

Supporting Document 2

Worcestershire Acute Hospitals NHS Trust

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No	Comments
1.	Does the implementation of this document require any additional Capital resources	No	
2.	Does the implementation of this document require additional revenue	No	
3.	Does the implementation of this document require additional manpower	Possibly	There is the potential for the number of requests to increase as a result of there no longer being a charge for the provision of information under GPDR
4.	Does the implementation of this document release any manpower costs through a change in practice	No	
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No	
	Other comments:	YES	Finance Department is aware of the cost associated with the loss of income recovered from charges applied previously under the Data Protection Act 1998

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval