Weston Area Health NHS Trust

GOV 22 Policy for Data Protection – Subject Access Requests
Version 4

Date Approved:	20 February 2018 This version (v4) effective from 25 May 2018.
Date for Review:	25 May 2021
Directorate / Department responsible (author/owner):	Corporate/Legal Services Manager/Sue Palmer
Contact details:	Wnt-tr.legalservices@nhs.net
Brief summary of contents	To implement the provisions of the General Data Protection Regulation ("GDPR") in respect of subject access requests.
Search criteria:	Data Protection, Subject Access Requests, GDPR
Executive Director responsible for Policy:	Director of Finance
Date revised:	January 2018
This document replaces (exact title of previous version):	Data Protection Act Policy – Subject Access Requests
Title and date of committee/forum/group consulted during development :	Health Informatics Committee 20 February 2018
Signature of Executive Director giving approval	Director of Finance
Intranet location:	Information Governance
Links to key external standards	IG toolkit
Related Documents:	None
Training Need Identified?	Yes – to be included in induction and refresher IG training.

Version Control Table

Date	V	Summary of changes	Author
01/10/10	1		Sue Palmer
01/03/13	2	Minor Amendments	Sue Palmer
01/03/15	3	Minor Amendments	Sue Palmer
25/05/18	4	Major revision to implement the provisions of the General Data Protection Regulation in respect of Subject Access Requests.	Sue Palmer

Document Amendment Form – minor amendments

No.	Date	Page no	Amendment	Authorised by
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Ten or less minor amendments can be made before the document is revised.

Major changes must result in immediate review of the document

If printed, copied or otherwise transferred from the Trust intranet, procedural documents will be considered uncontrolled copies. Staff must always consult the most up to date version – located on the intranet.

Table of Contents

1. Introduction and purpose

1.1 The Trust is a Data Controller and is registered with the Information Commissioner's Office ("ICO") under registration reference: Z5203570. The Trust collects and uses personal information about patients, staff, external contractor and others on a day to day basis.

1.2 The General Data Protection Regulation ("GDPR") came into effect on 25 May 2018. It superseded the Data Protection Act 1998. This policy details how the Trust will comply with its legal obligations under the GDPR in respect of subject access requests.

1.3 The GDPR legislates for the protection of personal information relating to living individuals. The Access to Health Records Act 1990 will remain relevant for health information relating to deceased persons.

1.4 Personal information is held by the Trust in a variety of media, such as information held on computers, memory sticks and CDs, written records and photographs. Personal identifiable data is any information that relates to an individual. It can be information relating to employees of the Trust or information held about patients and others. Sensitive data includes data about racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, genetic data and biometric data.

1.5 The key objectives of this policy and the associated subject access procedure (see appendix 1) are to ensure that personal information is processed in accordance with the GDPR, to meet the requirements of the Information Governance toolkit and to provide guidance on the correct way to handle requests for personal information.

2. Scope

2.1 This policy and the associated procedure applies to all employees of the Trust, including permanent, temporary and contract staff who come into contact with personal information.

2.2 All employees allocated responsibility for responding to subject access requests must be aware of the Trust's legal obligations.

2.3 Employees should be aware of the difference between the right of subject access under the GDPR ("what do you have on record about me?") and the general right to request information about the Trust generally under the Freedom of Information Act 2000 ("what information do you hold on this topic?") The Trust has a separate Freedom of Information policy.

2.4 This version supersedes any previous versions of this document.

3. Explanation of terms

3.1 GDPR – The General Data Protection Regulation which came into force on 25 May 2018 and has seven principles:-

3.1.1 Principle 1 – Lawfulness, fairness and transparency – Personal data must be processed lawfully and in a transparent manner in relation to the data subject.

3.1.2 Principle 2 – Purpose limitation – Personal data must be collected for specified, explicit and legitimate purposes.

3.1.3 Principle 3 – Data minimisation – Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.

3.1.4 Principle 4 – Accuracy – Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that incorrect personal data are erased or rectified without delay.

3.1.5 Principle 5 – Storage limitation – Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary.

3.1.6 Principle 6 – Integrity and confidentiality – Personal data must be processed in a manner that ensures appropriate security of the personal data.

3.1.7 Principle 7 – Accountability – The Trust shall be responsible for and be able to demonstrate compliance with the above six principles.

3.2 Subject Access requests – a request by an individual for information held by the Trust about them under the provisions of the GDPR.

3.3 ICO – The Information Commissioner's Office which is responsible for administering the GDPR and enforcing its provisions.

3.4 SIRO – The Trust's Senior Information Risk Owner, usually the Director of Finance, who is familiar with and takes ownership of the organisation's information risk policy.

3.5 Caldicott Guardian – who is responsible for ensuring that the Trust adheres to the Caldicott principles and is usually the Medical Director.

3.6 The Caldicott principles are as follows:-

3.6.1 Principle 1 - Justify the purpose(s) for using confidential information

3.6.2 Principle 2 - Don't use personal confidential data unless it is absolutely necessary

3.6.3 Principle 3 - Use the minimum necessary personal confidential data

3.6.4 Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

3.6.5 Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

3.6.6 Principle 6 - Comply with the law

3.6.7 Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

3.7 HIC – The Trust's Health Informatics Committee.

3.8 DPO – Data Protection Officer – Public authorities, such as the NHS, are required to appoint a DPO whose primary objective is to ensuring compliance with the GDPR.

4. Roles and Responsibilities

4.1 The role of the author

4.1.1 Ensuring the policy is required and does not duplicate standards of practice expected of professionals nor other local work, and for confirming the need with relevant line management or working group.

4.1.2 Ensuring that key stakeholders are consulted with and involved in the development of the document.

4.1.3 Ensure that the content of the procedural document is aligned with the requirements of the GDPR and other relevant regulation.

4.1.4 Undertaking an Equality Impact Assessment if required.

4.1.5 Following the agreed approval and ratification processes.

4.1.6 Ensuring the document is appropriately disseminated and communicated.

4.1.7 Describing how the procedural document will be monitored for compliance and effectiveness.

4.1.8 Where appropriate, ensuring implementation is carried out and retains evidence of the implementation.

4.1.9 Reviewing the document at the agreed interval.

4.1.10 Ensuring that documents comply with WAHT policies.

4.1.11 Ensuring that the governance record on the coversheet is complete and up-to-date. In cases where there is more than one author, all contributors should be recorded on the governance coversheet.

4.2 The role of the Health Informatics Committee (HIC)

4.2.1 Approving Information Governance procedural documents and recording discussion and approval in the minutes of the meeting. Approval is to be completed on the governance coversheet prior to the document being submitted to an Executive Director for authorisation.

4.2.2 Approving procedural documents relating to a department, service, team or professional group where it is not appropriate for these to be agreed locally.

4.7.3 Ensuring that all procedural documents submitted for approval comply with the Policy on Policies.

4.7.4 Ensuring that responsibility for developing a procedural document for a directorate, department or specialty, is assigned to the most appropriate person or team.

4.7.5 Ensuring local systems and processes comply with the Policy on Policies.

4.7.6 Providing a source of expertise and advice for staff developing Trust procedural documents.

4.3 The role of individual staff

4.3.1 Making themselves aware of and complying with this policy.

4.3.2 Alerting their line manager of any non-compliance with this policy where it is noted and represents an actual risk to the Trust, its staff, patients or the public.

5. Policy details

5.1 An individual who is the subject of personal information processed by the Trust has the right of access to this information, known as a subject access request. The procedure for dealing with subject access requests is set out at appendix 1. An individual is also entitled to receive confirmation as to whether his or her personal data are being processed and to be provided with supplemental information about the processing.

6. Dissemination and Implementation

6.1 This policy will be made available on the Trust's Document Management System (DMS) which can be accessed through the Trust's intranet.

6.2 The policy will form part of induction training for all new staff and will be included in the annual Information Governance refresher training.

6.3 The Trust's Communication Manager will assist in disseminating this policy by releasing to the Trust a regular list of all procedural documents recently published onto the document library via the Trust newsletter.

7. Monitoring Compliance and Effectiveness

7.1 This compliance with this policy will be monitored by the Legal Services Manager who manages the Subject Access Request team. Data will be provided on a quarterly basis to the Trust Board and the Health Informatics Committee.

Table 1 - Monitoring Compliance

Element to be monitored	**Number of subject access requests/compliance with the timescale set out in the GDPR**
Lead	Legal Services Manager
Tool	Audit of subject access requests spreadsheet
Frequency	Quarterly
Reporting arrangements	Trust Board and Health Informatics Committee
Acting on recommendations and Lead(s)	Health Informatics Committee/Legal Services Manager
Change in practice and lessons to be shared	Annual Information Governance refresher training

8. Reference and bibliography

General Data Protection Regulation

9. WAHT associated records

Nil

10. Staff compliance statement

All staff must comply with the Trust-wide procedural document and failure to do so may be considered a disciplinary matter leading to action being taken under the Trust's Disciplinary Procedure. Actions which constitute breach of confidence, fraud, misuse of NHS resources or illegal activity will be treated as serious misconduct and may result in dismissal from employment and may in addition lead to other legal action against the individual concerned.

11. Equality and Diversity statement

The Trust aims to design and implement services, policies and measures that meet the diverse needs of users of our services, population and workforce, ensuring that none are placed at a disadvantage over others.

Equality Impact Assessment Screening Tool

To be completed for any procedural document when submitted to the appropriate committee for approval.

		Yes/No	Rationale
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	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 there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the policy/guidance likely to be negative?	No	
5	If so can the impact be avoided?	No	
6	What alternatives are there to achieving the policy/guidance without the impact?	No	
7	Can we reduce the impact by taking different action?	No	
8	Actions identified following screening process	None	
9	Screening identified a full impact assessment.	No	

If you have identified a potential discriminatory impact of this policy/procedure, please refer it the appropriate Director in the first instance, together with suggested actions required to avoid/reduce this impact. For advice in respect of answering the above questions, please contact the H.R Department. For advice on completion of this form please contact the Governance Team.

Appendix 1

Procedure for responding to Subject Access Requests

1. Subject Access requests may be received by the Trust in various forms; by letter, email, fax, telephone or in person. Where requests are not made in writing (i.e. where requests are made over the telephone or in person) the requestor must confirm their application in writing or complete a Trust application form which is available on the Trust's external website www.waht.nhs.uk or upon request from the Legal Services Department.

2. When a subject access is received then it should be passed to the Legal Services, Access to Records team who are located in Brent Knoll building, unless it is in connection with HR records when it should be passed to the HR Manager in the Academy.

3. Upon receipt of the request all subject access requests are logged to ensure that the Trust has a complete record and that they are processed within the timescale set out in the GDPR i.e. within 30 days of receipt. Each request will be acknowledged and proof of identity of the requestor will be sought. Documents will not be released until the requestor's identity has been verified. A clinician will be asked to review the application and agree to the request. A clinician is entitled to request that some or all of the documents should not be disclosed if they would cause physical or mental harm to the requestor.

4. Some requests are made by third party agencies acting on behalf of the individual, for example by solicitors, Police, Social Services. These requests must be accompanied by a form of consent signed by the individual. If the patient lacks mental capacity then a request can be made by a party named on a Lasting Power of Attorney ("LPA") for Health and Welfare. If the request is made for a child then the consent form must be signed by a person with Parental Responsibility, unless the child is deemed to be competent to sign the form themselves. On rare occasions it may be possible to provide personal information to the Police or Social Services without the individual's consent, for example, if the request is in connection with a crime or safeguarding or if the Trust is in receipt of a Court Order. These requests must be approved by the Legal Services Department or the Trust's Caldicott Guardian (usually the Medical Director).

5. All documents must be reviewed before they are sent out. Any third party information must be redacted or consent of the third party must be obtained.

6. The documents must be provided within 30 days. This time scale can be extended by a further 2 months where requests are complex or numerous. If this is the case the individual must be informed within one month of the request and explain why the extension is necessary. If a subject access request is made electronically then the information should be provided in a commonly used electronic form (unless the requestor requires paper copies). The paper documents can be sent by Recorded Delivery using Royal Mail. The Post Room will provide the Tracking Number. Alternatively, the requestor can view the documents at Trust premises by arranging a mutually convenient appointment with Legal Services. The requestor must not be left alone with the original documents and must be accompanied by a member of the Legal Services department at all times.

7. If the requestor is unhappy with the way their Subject Access Request has been handled by the Trust they can contact the Trust's Data Protection Officer, Weston Area Health NHS Trust, Grange Road, Uphill BS23 4TQ for an internal review. Requestors who are not content with the outcome of the internal review have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner's Office can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF