OUR VALUES
Commitment
Care Quality

NHS
West Hertfordshire Hospitals
NHS Trust

Access to Health Records Disclosure Policy

Controlled document

This document is uncontrolled when downloaded or printed

Reference number	WHHT: G032
Document type	Policy
Version	5
Author's name & job title	Trisha McSkeane Head of Legal Services & Clinical Effectiveness
Department/Speciality	Legal Services Department
Division	Quality Governance
Reviewed by	PGRG
Review date	22 September 2020
Approved by PGRG	22 September 2020
Ratified by QSG	2 December 2020
Next review date	September 2023
Target audience	Access to Health Records; Legal Services Department staff; any Trust staff dealing with requests for access to records
Search terms	Access to Health Records, Disclosure, SAR
Previous document name (if different)	Access to Health Records Litigation and Claims Department Procedure

Contribution List

Key individuals involved in developing this version of the document

Name	Designation
Trisha McSkeane	Head of Legal & Clinical Effectiveness
Martina Brooker	Access to Health Records Officer
Stacey Newlan	Assistant Legal Services Manager

Change of History

Version	Date	Author	Reason for change
2.1	May 2011		Reviewed. Minor amendments made.
2	April 2009		Removed MVH Contact Details, Renamed Data Protection Manager to Information Governance Manager and additional responsibilities added. Additions to Monitoring & Review. Add 'Related Policies' section
3	May 2013		Reviewed. Additional guidance added to a number of sections to provide more detailed information
4	June 2015	Kate Hallam	Formal Review
5	Sept 2020	Trisha McSkeane	Formal review, update to Data Protection legislation

Abbreviations and Acronyms

Abbreviations and Acronyms	Description
MDT	Multidisciplinary Team
PGRG	Policy & Guideline Review Group
QSG	Quality & Safety Group

Contents

1. Introduction

Under the GDPR, living individuals or 'Data Subjects' have a right (subject to the payment of a fee, if applicable) to:

- Be informed whether Personal Data is being processed (which includes being held or stored)
- A description of the Personal Data held, the purposes for which it is processed and to whom the Personal Data may be disclosed
- A copy of the information constituting the Personal Data (subject to certain exceptions and conditions)
- Information as to the source of the Personal Data.

Requests for Personal Data will be known as 'Subject Access Requests (SAR's)'.

West Hertfordshire Hospitals NHS Trust is registered as a data controller with the Information Commissioner. As a data controller, the Trust acknowledges it has a duty in accordance with provisions of the GDPR to respond in a timely and appropriate manner to requests from living individuals or their authorised representatives to view or be provided with copies of the personal information held by the Trust about them.

An individual is entitled only to their own personal information, and not to information relating to other people (unless they are acting on behalf of that person).

Individuals have a right to see the information contained in personal data, rather than a right to see the documents that include that information. It is therefore acceptable to provide copies and relevant extracts of documents rather than original documents.

The Trust has 30 days from the date the SAR is received, in which to comply.

2. Objectives

To provide clear guidance to staff when dealing with a SAR in order to maintain the Trust's compliance with the GDPR; Data Protection Act 2018; Access to Health Records Act 1990 and other Trust policies.

3. Definitions

Data – recorded information, whether stored electronically on computer or in paper-based filing systems.

Data Controllers – individuals or organisations that hold and use personal information and that determine how and why the information is used.

Data Processors – individuals or organisations that process information on behalf of the Data Controller.

Data Subjects – the people the information is about and who can be identified from that information. All data subjects have certain legal rights in relation to their personal information.

Personal Data – the information about an identifiable living individual. This can be factual, such as name and address, or it can be an opinion about the individual.

Subject Access - The common term used to describe the right set out in section 7 of the GDPR which enables individuals to find out what personal data is held about them by a data controller, why it is held and who it is disclosed to.

4. Scope

This guidance has been written to assist all staff with a responsibility for dealing with requests for access to personal data, whether manual or electronic.

5. Responsibilities

The Trust has a corporate responsibility to establish and maintain staff guidance for access to personal records. The Trust will take all reasonable steps to identify, collate and provide copies of or access to all the personal information requested by an individual. It will only withhold information in circumstances where the disclosure of that information may breach the right to confidentiality of another individual or if another exemption to disclosure as described in the GDPR applies.

Head of Legal & Clinical Effectiveness responsible for updating this guidance in line with national and local guidance and legal obligations.

Access to Health Records Co-ordinators responsible for managing the process followed to provide responses to requests for access to medical records.

Legal Services Manager & Co-ordinators also responsible for managing the process followed to provide responses to requests for access to medical records from patients and their representatives bring claims against the Trust.

Radiology Clinical Systems Co-Ordinators hold the same responsibilities as the Access to Health Records coordinators in respect of patient requests for copies of Radiology scans.

Secretary/Administrator to Emergency Medicine Consultant Team holds the same responsibilities as the Access to Health Records coordinators in respect of patients or police requests for copies of ED records.

All Staff across the Trust should be aware of this policy and the Trust Information Governance policy as part of their own accountability for Information Governance.

6. Procedure

6.1 Subject Access

The right of access to health records is subject to a number of safeguards and exemptions which are designed to ensure the following:

- The identity of the applicant has been verified.
- Access is not given to any part of a record likely to cause serious harm to the physical or mental health of the patient or any other individual.
- Information is not released to a patient's personal representatives if it is evident that the patient did not wish access to be given.
- Third party information – access is not given to information which relates to or was provided by an individual (other than the patient) who could be identified from that information, except if the third party or other individual gives consent to the access.
- In the case of a deceased patient's representative, access shall not be given to any part of the record which is not relevant to any claim which may arise from the patient's death.
- A child, who (in the view of the appropriate healthcare professional) is capable of understanding what the application is about, can prevent a person with parental responsibility from having access to their records. Also, where in the view of the healthcare professionals, a child is not capable of understanding the nature of the application, the holder of the record is entitled to deny access if it were not felt to be in the child's best interest.

6.2 Request Received

All Subject Access Requests must be sent to:
Access to Health Records
Legal Services Department
Admin Block
Watford General Hospital
WD18 0HB

or emailed to: wherts-tr.accesstohealthrecords@nhs.net

6.3 Datix

A Datix will be opened on the Claims Datix module to track the request through the Trust detailing the date that stages are completed.

Copies of relevant correspondence or documentation in connection with the Subject Access Request will be scanned and saved on Datix.

6.4 Identity

To comply with the law, a Subject Access Request may only be made by the Data Subject, or someone who has their written consent to receive the Personal Data requested. Where the Data Subject is a child, see section 8.1 as to when a parent or person with parental responsibility may make a Subject Access Request on a child's behalf.

Adequate steps must be taken to identify the Applicant before commencing the work to comply with the Subject Access Request under the GDPR.

Examples of suitable documentation to prove identity could include **copies** of:

- valid passport
- driving licence
- birth certificate, along with
- some other proof of address, e.g. a named utility bill.

Copies of evidence of identity should be confidentiality disposed of once the necessary checks have been made.

6.5 Viewing a Record

Arrangements for viewing a record will be made between the patient/requester and the Access to Health Records co-ordinator once they have undertaken initial administration of the request.

Access will be supervised by the Access to Health Records co-ordinator who will ensure that the record remains safe. The co-ordinator must not comment or advise on the content of the record. If the applicant raises queries these will be recorded and provided to a healthcare professional to prepare a written response, or to arrange a further meeting with the healthcare professional present.

6.6 Time limits

There is a 30 day time limit to comply with the request. The 30 days begins from the receipt of satisfactory proof of identity and payment, if applicable. The clock may be stopped if there is any delay in receiving details essential to the search for the correct records. Department of Health policy is 21 days although this is not a legal obligation.

6.7 Search of Data Files

The Data Owners will be responsible for checking systems and files for any reference, directly or indirectly, relating to the Data Subject. Copies of the Personal Data will be obtained and returned to the Designated Person dealing with the request.

Requests can include copies of information contained on Trust servers in the form of folders, files and emails between Trust staff. Requests of this nature will be handled by the Information Governance Manager.

Important: ***Where Personal Data contains information as to the physical or mental health or condition of the Data Subject e.g. Medical Records or Occupational Health records, then disclosure cannot be made without reference to an appropriate healthcare professional*.**

The health professional that is appropriate will be the person currently or most recently responsible for the clinical care of the Data Subject to which the information relates or, where more than one health professional is involved, then the one most suitable to advise on these matters.

Should any Personal Data be found which might need to be withheld because it would:

- identify another individual and it would be unreasonable in the circumstances to do so or,
- cause serious harm to the physical or mental health or condition of the Data Subject, or any other person, or
- which you otherwise have concerns about disclosing (although under the GDPR such Personal Data may still have to be disclosed) contact the Trust Information Governance Manager or Head of Legal Services immediately for guidance.

6.8 Collating Responses

The Access to Health Records coordinator will collate the Personal Data received and prepare the disclosure response to the Applicant as necessary.

Should any information contained in the Personal Data of the Data Subject identify another individual then that information should be withheld or redacted, unless either of the following circumstances applies:

- the other individual has consented to the disclosure of the information, or
- if it is reasonable in all the circumstances to comply with the request without the consent of the other individual. Seek additional advice from Information Governance Manager or Head of Legal in these circumstances.

Note: Access to records should not be refused where this other individual is a health professional who has compiled or contributed to the health record or has been involved in the care of the Data Subject, unless serious harm to that health professional's 'physical or mental health or condition may result from such disclosure'.

6.9 Sending Copies of Data

When the Personal Data to be disclosed to the applicant is complete and agreed by the appropriate healthcare professional, copies of that personal data and a covering letter will be sent to the applicant.

Where possible, data should be encrypted before disclosure and be sent by recorded delivery. Unencrypted data must be collected in person by the Data Subject or posted by Special Delivery.

6.10 Informal Access to Health Records

Patients, during or at the end of their treatment, are entitled to ask what has been recorded about them, during that episode of care.

A request of this nature does not need to be in writing. Patients may be allowed to see this part of their records at the discretion of the appropriate health professional, and be given an explanation of any terms to assist understanding.

The appropriate healthcare professional is the person principally responsible for their clinical care and often will be a consultant, but may also be a nurse.

6.11 Access to Health Records of Deceased Persons

Health records relating to deceased people are not covered under the DPA or GDPR. However, it is Department of Health policy that these records should be treated with the same level of confidentiality as those relating to a living individual.

Access to the health records of a deceased person is governed by the Access to Health Records Act 1990. Under this legislation when a patient has died, their personal representative or executor or administrator, or anyone having a claim resulting from the death (this could be a relative or another person), has the right to apply for access to the deceased's health records.

For access to records relating to the deceased, applications may be received from:

- the deceased's personal representative, or
- any person who may have a claim arising out of the deceased's death.

However access is **NOT** to be given to the record or any part of it if any of the following apply:

- a note is included in the record, that the deceased did not wish access to be given
- the deceased had given the information and would not have expected it to be disclosed
- it would disclose information that is not relevant to any claim, or
- it would disclose information about a third party.

If appropriate, information would be required to establish a link between the Applicant and the deceased. A copy of the death certificate and a description as to the relationship with the person making the request or valid reason for access should be sought, together with proof of identity of the Applicant.

7. Monitoring & Compliance

1	Following local and national policies and guidelines, what key elements require monitoring?	List elements to be monitored	Compliance against 30 day response requirement
2	Who will lead/be accountable for monitoring?	Lead title and/or MDT	Head of Legal & Clinical Effectiveness
3	Describe how the key elements will be monitored?	List tools to evidence compliance	Datix /Excel

4	How frequently will each element be monitored?	List frequency of monitoring for each element	Quarterly, and included in Annual Claims & Inquests report
5	Explain the protocols for escalation in the event of problems?	List the processes of escalation	Follow section 6 in this policy
6	Which Committee/ Panel/ Group will reports go to?	List the Committee/Panel/ Group/Peer Review that the reports will go to	Quality & Safety Group
7	Explain how the policy/guideline will be disseminated within the Trust?	List ways identifying how this document will be shared and how it will be recorded that appropriate staff have been made aware of the document and where to find it	The policy will be published on the Trust's Intranet

8. Disclosure – other than directly to the Data Subject

Personal Data may be requested by third parties, e.g. solicitors, on behalf of the Data Subject. Where this is accompanied by authorisation from the Data Subject then this request can be processed using the procedure for Subject Access Requests.

Where necessary the third party should be contacted for additional details required to enable an effective search for the Personal Data required for their purpose.

No disclosure to a third person should be made unless authorisation is obtained from the Data Subject or the request is for crime or taxation purposes or it is otherwise permitted under the GDPR. Seek additional advice from the Information Governance Manager or Head of Legal Services in these circumstances.

In some instances a medical practitioner will request further information where a patient has been referred to him. Such a request for information should be referred to the healthcare professional responsible for the patient's clinical care.

9. Police Requests

Requests from the police must be accompanied by a section 29 notice signed by a senior officer, unless they provide a signed consent from the Data Subject. The section 29 notice should explain:

- What records they need (only the minimum should be released)
- Why they need the information.

If there are any concerns, the police must be required to produce a Court Order.

10. Regulatory Bodies (e.g. GMC, NMC)

Schedule 2, Part 1, Paragraph 7 of GDPR provides an exception to the duty to notify the data subject their personal data is being processed if it is likely to prejudice the proper discharge of a regulatory function. Only relevant records should be disclosed.

11. Attorneys

An individual acting under a Lasting Power of Attorney can ask to see information relevant to the decisions the attorney has the legal right to make. Health information can also be shared with a person holding a Power of Attorney if it is in the patient's best interests. If the Attorney does not have a clear right to disclosure they can apply to the Court for an Order for disclosure.

12. References

- GDPR – General Data Protection Regulations (2018)
- Data Protection Act 2018
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Caldicott Principles
- ICO Subject Access code of Practice

13. Related Policies and Guidelines

- Health Records Management Policy
- Records Retention and Disposal policy
- Data Protection 2018 Policy
- Information Governance Management Framework

14. Equality Impact Statement (EIA)

What is an equality impact assessment?

There are many benefits in conducting an equality impact assessment (EIA) prior to making business decisions about policies, clinical guidelines or any other work that may potentially impact on a wide range of people with protected characteristics. Equality impact assessments should not be seen as an afterthought once decisions have already been made.

Benefits:

- Improved capacity to consider equality, diversity and inclusion as part of business management
- Reduced costs as a result of not having to revisit a policy/project
- Take into account a diverse range of views and needs
- Enhanced reputation as a Trust that is seen to understand and respond positively and proactively to diversity.

Whatever approach you take to an equality impact assessment, case law has established that you should keep an accurate, dated, written record of the steps you have taken to analyse the impact on equality. This will help you to check whether you are complying with the duty and it will be useful if your decisions are challenged.

When completing an equality impact assessment you should consider:

- Treating a person worse than someone else because of a protected characteristic (known as direct discrimination)
- Putting in place a rule or way of doing things that has a worse impact on someone with a protected characteristic than someone without one, when this cannot be objectively justified (known as indirect discrimination)
- Treating a disabled person unfavourably because of something connected with their disability when this cannot be justified (known as discrimination arising from disability)
- Failing to make reasonable adjustments for disabled people.

Equality impact assessment process

Stage 1 (Screening)

This stage provides an opportunity to explore whether the policy decision may have a negative, neutral or positive impact on different groups of people.

- If yes, use the ‘comments’ column to describe what this impact could be.

- If no, outline how have you arrived at this conclusion.

- If unsure use the ‘comments’ column to describe what you need to do to find out.

Stage 2 (Full Assessment)

This should be carried out in compliance with policy HR028 Equality & Human Rights Policy.

Equality Impact Statement (EIA)

Does this policy/guideline affect one group less or more favourably than another on the basis of:				
				Comments
1	Age (younger people & children& older people)		no	
2	Gender (men & women)		no	
3	Race (include gypsies and travellers)		no	
4	Disability (LD, hearing/visual impairment, physical disability, mental illness)		no	
5	Religion/Belief		no	
6	Sexual Orientation (Gay, Lesbian, Bisexual)		no	
7	Gender Re-assignment		no	
8	Marriage & Civil Partnership		no	
9	Pregnancy & Maternity		no	
	Is there any evidence that some groups maybe affected differently?		no	
	Could this document have an impact on other groups not covered by a protected characteristic? (e.g.: low wage earners or carers)		no	
	If '**NO IMPACT'** is identified for any of the above protected characteristics then no further action is required.			
	If '**YES IMPACT**' is identified a full impact assessment should be carried out in compliance with HR028 Equality & Human Rights Policy and linked to this document			

Any other comments:
Please use this box to add any additional comments relevant to the assessment

Assessment completed by:	Trisha McSkeane, Head of Legal & Clinical Effectiveness	Date completed:	02/09/2020

If you have any queries or concerns about completing the EIA form, contact the Trust's Inclusion & Diversity Team at WestHerts.Inclusion@nhs.net