

MHC

Subject Access Request Policy 2023

Name of policy:	Subject Access Request Policy
Date valid from:	18 April 2023
Date to be reviewed:	This policy will be reviewed in 2 years. Earlier review may be required in response to relevant changes in legislation or guidance.

CONTENTS

	Page
1. Introduction	3
2. Recognising a Subject Access Request (SAR)	3
3. Dealing with a Subject Access Request (SAR)	4
4. Redacting data	5
5. Refusing requests	6
6. Fees	6
7. Access to records of deceased individuals	6
8. References	7
Appendix 1 – Request for access to staff records	8
Appendix 2 – Request for access to patient or resident records	10

1. INTRODUCTION

- 1.1 Individuals have the right under the General Data Protection Regulation (GDPR), subject to certain exemptions, to have access to their personal records that are held by MHC UK. This is known as a 'subject access request' (SAR). Requests may be received from members of staff, patients, people acting on behalf of patients or any other individual who MHC UK has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.
- 1.2. The General Data Protection Regulation applies only to living persons but there are limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990 (see section 7 below).
- 1.3. MHC UK has developed this policy to guide staff in dealing with Subject Access Requests that may be received.

2. RECOGNISING A SUBJECT ACCESS REQUEST (SAR)

- 2.1 A subject access request (SAR) is simply a request made by or on behalf of an individual for a copy of information held about them by MHC UK. The General Data Protection Regulation (GDPR) entitles all individuals to make requests for their own personal data. A request may be made by
 - the person that the data is about (the data subject);
 - a representative of the data subject who has their written consent such as a solicitor;
 - a person who has been appointed by the Court of Protection;
 - a person with enduring Power of Attorney;
 - a person appointed as an Independent Mental Health Advocate under the Mental Capacity Act 2005.The above list is not exhaustive.
- 2.2 The request does not have to be in any particular form or media nor does it have to include the words 'subject access' or make any reference to the General Data Protection Regulation (GDPR). A SAR may be a valid request even if it refers to other legislation and should therefore be treated as a SAR in the normal way.

- 2.3 The person making the request does not have to tell you the reason for making the request or what they intend to do with the information, although it may help us to find the relevant information if they do explain the purpose of the request.
- 2.4 The following are some of the more common types of requests received:
- I would like a copy of all the information you hold about me in my HR file
 - I would like a copy of my medical notes
 - I am a solicitor acting on behalf of my client and request a copy of his medical records. A signed authority is enclosed.
- 2.5 Requests may sometimes be received from the Police or HMRC for the following purposes:
- The prevention or detection of crime;
 - The apprehension or prosecution of offenders;
 - The assessment or collection of tax or duty.

The request should be signed by a senior officer from the relevant authority. The request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

3. DEALING WITH A SUBJECT ACCESS REQUEST (SAR)

- 3.1 All staff should be aware of how to deal with a SAR as the request may be received by any department. An acknowledgement that the request has been received should be sent within 3 working days. The request should include as much information as possible about what exactly is being requested. In some cases, we may need to seek clarification in order for us to narrow down our search and to respond to the request.
- 3.2 Proof of ID may be required from the person making the request plus a valid signed authorisation where they are making a request on behalf of an individual.
- 3.3 Under GDPR, the information requested must be sent within one month of receiving a valid request. Decisions about what information can be provided in response to a SAR should be made by a senior member of staff with sufficient knowledge of current data protection regulations. See section 4 below where the request involves clinical data or third party data which may need to be redacted.
- 3.4 Before copies of the requested documents are given to or sent out to the person making the subject access request, a check should be carried out by two suitable members of staff to confirm that the documentation is in order and is 'good to go'. The check should be recorded and dated.

- 3.5 A record should be maintained of all requests received, detailing
- date received
 - applicant's details
 - information requested
 - who is dealing with the request
 - information provided
 - any information not provided and the reasons why
 - in what format the information was provided and how eg paper copies by special delivery, encrypted email etc.
 - date that the request was finally responded to
- 3.6 The person dealing with the request should satisfy themselves as to the validity of the request. This may require confirming and verifying the identity of the applicant and/or the data subject or confirming that they are authorised to act on behalf of the data subject.

4. REDACTING DATA

- 4.1 All requests for clinical data should be reviewed by a suitable clinician. Where it is considered that there is information held which, were it to be provided to the patient or resident, is likely to cause serious harm to the mental or physical health of that individual or others then this information must not be provided. The final decision as to what information to provide and what not to provide should be made by a senior clinician such as the Caldicott Guardian. See the Information Governance policy for further information about the role of the Caldicott Guardian and the Caldicott Principles.
- 4.2 When personal records contain details of third parties, all references to third parties must be removed, redacted or blanked out unless consent has been obtained by them for their details to be released. Please note that this does not normally apply to health professionals.

5. REFUSING REQUESTS

- 5.1 There are times when requests by individuals for access to personal information can be refused, for example where providing the information
- would be likely to prejudice any of the following:
 - Prevention or detection of crime;
 - The apprehension or prosecution of offenders;
 - The assessment or collection of any duty or tax;
 - Confidential references given by the data controller;
 - Legal professional privilege;
 - would result in self incrimination;
 - where there is a statutory or court restriction on disclosure eg adoption records;
 - in respect of confidential references provided by us.

6. FEES

- 6.1 Under GDPR, information provided in response to a SAR must be provided free of charge. However, a 'reasonable' fee can be charged when the request is manifestly unfounded or excessive, particularly if it is repetitive. Any fee charged can only cover administrative costs.

7. ACCESS TO RECORDS OF DECEASED INDIVIDUALS

- 7.1 The Common Law Duty of Confidentiality extends beyond death. Certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:
- The patient's personal representative (ie Executor or Administrator of the deceased's estate)
 - Any person who may have a claim arising out of the patient's death
- 7.2. A next of kin has no automatic right of access to a deceased relative's records but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from a suitable clinician in relation to requests for deceased records.

8. REFERENCES

Subject Access Code of Practice, Information Commissioner's Office:

<https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf>

CCTV Code of Practice, Information Commissioner's Office:

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>.

Overview of the General Data Protection Regulation, Information Commissioner's Office:

<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>

Please return completed forms by post or email to:

The Data Protection Officer, MHC (UK)

Alexander House, Highfield Park

Llandyrnog, Denbighshire LL16 4LU

Email: DPO@mhc-uk.com

Appendix 1

General Data Protection Regulation

Request for Access to Employment/Personnel Records



MHC

1. Staff's details

First name(s):
.....

Surname:
.....

Date of birth:
.....

Address:
.....

Postcode:
.....

Contact phone number:
.....

Email:
.....

Payroll Number (if known):
.....

2. Please tell us what information you are asking for

Please be as specific as possible about exactly what information you are asking for and over what period.

Appendix 1

3. Details of the person making the request if you are not the person named above

First name(s):

Surname:

Address:

Postcode:

Contact phone number:

Email:

Your relationship to the person named in part 1 above:

DECLARATION

I declare that the information given by me is correct to the best of my knowledge and that I am applying for access to the above records in the following capacity:

I am the employee

I am acting on behalf of the employee and attach the employee's signed authorisation

I am the employee's legal representative or have been appointed by the Court to act on their behalf and attach proof of my appointment

Signed:

Date:

Appendix 2

General Data Protection Regulation Request for Access to Records of Patients or Residents



MHC

1. Details of the patient or resident whose information is being requested (the data subject)

First name(s):
.....

Surname:
.....

Date of birth:
.....

Address:
.....

Postcode:
.....

Tel No:
.....

Mobile:
.....

Email:
.....

NHS Number (if known):
.....

2. Details of the person making the request if you are not the person named above

First name(s):
.....

Surname:
.....

Address:
.....

Postcode:
.....

Tel No:
.....

Mobile:
.....

Email:
.....

Your relationship to the person named in part 1 above:
.....
.....

Appendix 2

3. Please tell us what information you are asking for

Please be as specific as possible about exactly what information you are asking for and over what period. This will enable us to deal with your request more quickly.

DECLARATION

I am a current patient or resident

I am a former patient or resident *(Please provide proof of ID such as driving licence or passport plus two recent utility bills)*

I am acting on behalf of the patient or resident *(please provide signed authorisation)*

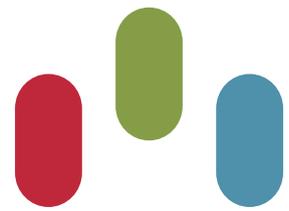
I am the patient or resident's legal guardian or have been appointed by the Court to act on their behalf *(Please provide valid documentation as proof)*

I am the deceased person's personal representative *(Please provide proof of your appointment)*

I have a claim arising from the death of the patient or resident and wish to access information in pursuit of my claim *(Please provide proof of ID such as driving licence, passport plus a recent utility bill and details of the claim)*

Signed:

Date:



MHC

Please return completed forms by post or email to:

The Data Protection Officer, MHC (UK)

Alexander House, Highfield Park

Llandyrnog, Denbighshire LL16 4LU

Email: DPO@mhc-uk.com