**ACKLAM MEDICAL CENTRE**

**SUBJECT ACCESS REQUEST POLICY**

**Version : 4**

**Author : Catherine Thomas**

**Date : 26/03/21**

**Review Date : 26/03/22**

**Introduction**

The General Data Protection Regulation (GDPR) provides Data Subjects the right, subject to certain exceptions, to view and or obtain a copy of all personal data that a Data Controller holds about them. These requests are known as Subject Access Requests (SAR) and apply to personal information relating to living individuals held in computerised or manual formats irrespective of when they were created.

Access to deceased patient’s information is governed by the Access to Health

Records Act 1990.

This policy describes the process embedded within the practice when responding to a Subject Access Request received either under GDPR or the Access to Health Records Act 1990.

**Scope**

This policy applies to all requests received from patients and staff for access to

personal data which the practice holds about them regardless of the format in which

that data is held in. It also applies to requests received from others for access to personal data of the deceased.

**Purpose**

The purpose is to provide guidance to staff involved in the handling and processing

of ‘Subject Access Request’ received under GDPR or the Access to Health Records Act 1990.

**Objectives**

The objectives of this Policy are to:

* Ensure the practice meets its obligations regarding ‘subject access requests’

under the terms of GDPR and the Access to Health Records Act 1990;

* Set out clear guidelines for staff to help make the access timely and within

the legislation laid down by Government;

* Ensure staff are aware of their responsibilities in the management of access

to records.

**Definitions**

**Personal Data**

The provisions of GDPR apply only to personal data. The term ‘personal data’ is defined, as data, which relate to a living individual who can be identified

from those data, or

from those data and other information which is in the possession of,

or is likely to come into the possession of, the data controller

and includes any expression of opinion about the individual and any indication of

the intentions of the data controller or any other person in respect of the individual.

**Health Record**

A ‘health record’ is defined in the Act as being any record which consists of

information relating to the physical or mental health 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.

A health record can be computerised (electronic) and/or manually held. They may

include such documentation as hand-written clinical notes, letters to and from other

health professionals and laboratory reports, and other imaging records, printouts/photographs.

**Health Professional**

A health professional is defined in GDPR as:

a registered medical practitioner;

a registered dentist as defined by section 53(1) of the Dentists Act

1984;

a registered optician as defined by section 36(1) of the Opticians Act

1989;

a registered pharmaceutical chemist as defined by section 24(1) of

the Pharmacy Act 1954 or a registered person as defined by Article

2(2) of the Pharmacy (northern Ireland) Order 1976;

a registered nurse, midwife or health visitor;

a registered osteopath as defined by section 41 of the Osteopaths

Act 1993;

a registered chiropractor as defined by section 43 of the

Chiropractors Act 1994;

any person who is registered as a member of a profession to which

the Professions Supplementary to Medicine Act 1960 for the time

being extends;

a clinical psychologist, child psychotherapist or a speech therapist;

a music therapist employed by a health service body;

**Parental Responsibility**

Parental responsibility is defined in the Children Act 1998 as ‘all the rights, duties,

powers, responsibilities and authority which by law a parent of a child has in

relation to the child and his property’. A person with parental responsibility is:

the natural mother;

the natural father, if married to the mother either before or after the

birth, even if divorced or separated;

the natural father, if unmarried, and he registered the birth along with

the mother from 1 December 2003;

the natural father, if unmarried, by agreement with the mother

(evidenced by a form provided by a solicitor, signed by both parents

and witnessed by a Officer of the Court) or by a court order (parental

responsibility order);

the natural father, if unmarried, and appointed as the child‟s guardian

on the death of the natural mother;

Same sex partners if civil partners at the child‟s birth or formal

parental agreement;

an individual (generally a family member) with a residence order for

the child (if the order is for a period of time, then parental

responsibility is removed at the end of the period);

an individual who has legally adopted the child;

a local authority under a care order – individual acting as a Children‟s

Guardian.

Person who has an emergency Protection Order.

**Information Commissioner**

The Information Commissioner‟s Office (ICO) is a UK independent supervisory

authority reporting directly to parliament. They oversee and enforce compliance

with both the GDPR, Data Protection Act 1998 and Freedom of Information Act 2000. The ICO also publish guidance & information to encourage organisations to achieve good practice and help the general public understand their rights.

**Legislation**

The main legislative measures that give rights of access to health records and

personal identifiable information include:

***GDPR***

GDPR regulates the processing, including the disclosure, of information about identifiable living individuals, subject to specified exemptions.

GDPR gives individuals (known as data subjects), or their authorised

representative, the right to apply to see certain personal data held about them,

including health records. These rights are known as ‘Subject Access Rights’.

Data Protection legislation is not confined to health records held for NHS purposes

and includes all information identifying and relating to living individuals.

***The Access to Health Records Act 1990***

The Access to Health Records Act 1990 (AHRA) regulates the processing,

including the disclosure, of information about identifiable individuals that are

deceased. The Act states that only two groups of people may access the patient’s

health records:

the patient’s representative (executor or administrator of the estate) or

anyone with a claim arising out of the patient’s death

In order to show that the applicant has been appointed as the personal

representative the practice will ask for a copy of the Grant of Probate or Letters of

Administration.

The personal representative need give no reason for applying for access to a

record. However, disclosure to a personal representative is prohibited if there is a

statement in the patient’s records that they do not wish disclosure to be made to

that person. Individuals other than the personal representative have a legal right of

access under the Act only where they can establish a claim arising from a patient’s

death. Their right is restricted to information ‘relevant to the claim’.

There is less clarity regarding which individuals may have a claim arising out of the

Patient’s death. Whilst this is accepted to encompass those with a financial claim,

determining who these individuals are and whether there are any other types of

claim is not straightforward. The decision as to whether a claim actually exists lies

with the record holder. In cases where it is not clear whether a claim arises the

practice will seek legal advice.

**Roles & Responsibilities**

**Management Partner**

The management partner holds overall responsibility for Subject Access Request, but on a day-to-day basis will be delegated to admin staff who are trained to deal with access to health record requests

**All Clinicians**

All clinicians are responsible for ensuring that:

health records are maintained to the highest standards ensuring that

content is legible, accurate, comprehensive and understandable;

maintaining an awareness of confidentiality and record keeping

standards including patients’ rights of access to their health records, and

the implications that this has on current record keeping practices.

**Relevant Clinician**

The ‘relevant clinician’ would normally be the individual who is or was responsible

for the clinical care of the patient during the period to which the application refers

and has the following responsibilities:

For third party access requests

assessing the capacity of the patient to consent to the disclosure of their

health records to that third party;

checking if the patient lacks capacity whether the patient has at any time

indicated a wish not to give access to all or part of the record;

deciding for incapacitated patients whether disclosure is in their best or

vital interests and whether disclosure outweighs the obligations of confidentiality to the individual and broader pubic interest in the provision of a confidential service.

For all requests

checking if any part of the health record, if disclosed, is likely to cause

serious harm to the physical or mental health condition of the Data

Subject or any other person;

signing off information within the health record as being fit to disclose to

the requester

**Admin staff responsible for Access to Health Record requests**

The Access to Health Records Administrator is responsible for;

* coordinating subject access requests while ensuring they are responded
* to correctly in accordance with statutory requirements.
* recording applications received onto the patient records
* Logging requests on the spreadsheet shared securely on the practice shared drive.
* locating all relevant information relating to the request.
* checking if any part of the health record discloses information relating to

another individual, or information provided by a third party, who can be

identified from the entry (unless that person has consented to its disclosure, or is a health professional involved in the care of the patient).

* acting as a reference point for procedures and complaints as detailed in

this policy.

**Managers**

ensuring Subject Access Requests are responded to correctly in

accordance with statutory requirements.

locating all relevant information relating to the request.

identifying where additional personal information may be held within

the Trust that may assist in the request that may not be recorded in

the individuals personnel file.

**Employees**

All employees must understand their duty of care to ensure the confidentiality of all

personal data. In addition they must have an understanding of this policy and

where to direct individuals enquiring about subject access requests.

**Types of Requester**

A Subject Access Request is usually received by the following applicants:

**The Patient**

Patients are entitled to make a request in writing to see any personal data held

about them under GDPR

**A Person Acting on the Patients Behalf**

A person acting on the patient’s behalf (e.g. a relative or carer) may apply for a

copy of the patient’s records – however they must have obtained informed, explicit

and written consent from the patient, have lasting Power of Attorney, or be an

Independent Mental Capacity Advocate (IMCA). An individual acting under a

Lasting Power of Attorney can only have disclosure of information relevant to the

decisions the attorney has the legal right to make.

**Children & Adolescents**

If the application for access to a child’s record, a person under the age of 16, is

made by someone having parental responsibility access shall only be given where:

the child is capable of understanding what the application is about

and has consented to it;

the child is not capable of understanding the nature of the application

and giving access would be in his/her best interests. The relevant

clinician will decide on the childs capacity to understand the application.

Legally, young people aged 16 and 17 are regarded to be adults for the purposes

of consent to treatment and the right to confidentiality. As such, if a patient of this

age wishes a professional to keep aspect of treatment confidential, this wish

should be respected.

Children under the age of 16 who have the capacity and understanding to take

decisions about their own treatment are entitled to decide whether personal

information may be disclosed. Case law has established that such a child

identified in Fraser Guidelines (previously known as ‘Gillick Competent’), i.e. where

a child is under 16 but has sufficient understanding in relation to the proposed

treatment to give or withhold consent, consent or refusal should be respected.

However, good practice dictates that the child should be encouraged to involved

parents or those with parental responsibility in their treatment.

If an individual is claiming parental responsibility then they must provide a copy of

the necessary evidence such as a parental responsibility order or birth certificate.

**Solicitors or Insurance Companies**

Where a solicitor, lawyer or other legal professional requests access on behalf of a

client they are representing, the signed consent of their client must be obtained

and evidenced. The request must be dealt with in the same way as if it had come

direct from the patient.

**Government Benefit Agencies**

Requests for information may be made by:

Department of Work and Pensions

Veterans Agency

Criminal Injuries Compensation Authority

The Trust will require written consent from the patient for the release of copies of

Heath Records

**Other Health Care Providers**

Other healthcare organisations (NHS and private) may request copies of a

Patient’s record in order to provide continuity of care for that patient.

**All other requests including those from the police**

Although not immediately apparent, these requests are made under the Data

Protection Act 1998. When made on behalf of a victim of crime they must meet the same requirements listed above i.e. the request must contain the original written request and/or authority, signed by the applicant, for the release of their records to the police and the applicant’s authority for them to act on their behalf.

Section 29 of the Act provides exemptions from the first Data Protection Principle

for;

the prevention or detection of crime,

the apprehension or prosecution of offenders, or

the assessment or collection of any tax or duty or of any imposition of a

similar nature,

and section 35 provides exemptions from the non-disclosure provisions of the Act;

where the disclosure is required by or under any enactment, by any rule of

law or by the order of a court; or

where the disclosure is necessary

* for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
* for the purpose of obtaining legal advice,
* or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

In the event of any such requests where consent has not been sought and

provided, the requester e.g. Police, HM Revenue and Customs, Local Counter

Fraud Specialist, NHS Protect, Nursing and Midwifery Council must be referred

direct to Caldicott Guardian, Dr Pauline De Jongh.

**Records of Deceased Patients**

Health records relating to deceased patients will be treated with the same level of

confidentiality as those relating to living people. Under the Access to Health

Records Act 1990 a request to see a deceased patient’s health record or to have a

copy thereof can be made by the patient’s personal representative or any person

who may have a claim arising out of the patients death.

The personal representative – who may be a relative, friend or solicitor or anyone

having a claim resulting from the death has the right to apply for access to the

relevant part(s) of the deceased’s health record under the ‘Access to Health

Records Act 1990’. Where the requestor is not acting in a legal capacity, they

should detail why they need access in pursuing a claim. Where they are the

executor or administrator they must provide proof of appointment under the

Will/Grant of probate.

**Staff (including ex-employees)**

Any member of staff or ex-employee wishing to obtain copies of personal

information about them will need to make a written request to the management partner, Catherine Thomas. The request should document exactly what information is required and where appropriate specify dates. Information held within a personal file or in the form of an email may consist of a mixture of information that is an individuals personal data, is third party personal data and that isn’t personal data at all. For information to be personal data it must *relate to* an individual and allow an individual to be *identified* from it. The context in which information is held, and the way it is used, can also have a bearing on whether it *relates* to an individual and therefore on whether it can be the individual’s personal data.

Information held may also record an individual’s opinion of something or another

and calls for careful judgement to determine whether an opinion relates to the

person who holds it or relates to the person or issue the opinion is of, or both.

**Guidelines on the Procedure**

The following procedure relates to Subject Access Requests for access to Health

Records only.

Written Applications

Applications must be made in writing to the management partner, Catherine Thomas.

**Determine Validity of Applications**

All applicants must provide proof of identity (driving license, passport or birth

certificate), and proof of address (utility bill or bank statement).

**Administration Fees**

Applications can be divided into two groups – applications from solicitors or

insurance companies on behalf of clients and applications direct from patients or

other data subjects. In all cases the practice will not charge for copy records unless the request is felt to be unreasonable. If the request is deemed unreasonable the practice reserve the right to seek advice from the ICO on what is deemed reasonable. This may result in the negotiation of an admin fee or extension of time to complete the request.

**Denial of Access**

Access to all or part of a health record will be denied if;

in the opinion of the relevant clinician, the information to be disclosed would be likely to cause serious harm to the physical or mental health or the applicant or another person

data recorded in the file supplied by a third party, who is not a health professional involved in the treatment or care given to the data subject, i.e. the data subjects family or friends and from whom no specific consent for disclosure is held.

data processed for any crime and taxation purposes where the provision of this information would be likely to prejudice any of the crime and taxation purposes.

data processed for the purposes of national security.

data processed for the purposes of research, historic record or

statistical purposes that will not cause distress to any data subject or

is anonymised.

the health record of a deceased person where the patient’s express wish not to disclose is recorded or the information is not relevant to any claim arising from the patients death.

the relevant clinician in charge considers that the patient authorising access to another individual has not understood the meaning of the authorisation

**Timetable for Access**

For living individuals, GDPR superseded the Access to Health Records Act 1990. The Access to Health Records Act 1990 required requests to be complied with within 21 days where the record has been amended within the previous 40 days, where as GDPR requires requests to be complied with within 30 days.

**Inaccuracies in Health Records**

Any inaccuracies in the record, to be corrected at the request of the applicant will

only be made in agreement with the relevant health care professional in charge. If

the relevant clinician does not agree with the request a note recording the matters

alleged to be inaccurate will be made on the record and a copy sent to the

applicant.

**Sending Copies of Records**

Copies of records sent externally in the post should be:

In a sealed tamper proof envelope (e.g. self sealing jiffy bag)

Addressed to a named person

Marked ‘Private and Confidential’

To be opened by Addressee only

Sent by special delivery only

Copies must **not** be sent via fax or by e-mail

Copies of records sent internally must be:

In a sealed, tamper-proof envelope (e.g. self sealing jiffy bag)

Addressed to a named person

Marked ‘Private and Confidential’

**Sending Original Records**

Original health records must not be sent to any applicant (including solicitors)

because of the potential detriment to patients and the practice if the records are lost.

**History and Completion of Requests**

A record of the request, its current status and completion will be recorded in line

with Information Governance requirements. This information will be recorded and

maintained by the SAR admin team. A note of what information was supplied to the applicant together with any comment will be retained electronically.

**Complaints Procedure**

Should an individual have any query or disagreement with any decisions made

regarding a data subject access request, or should they have any disagreement

with the information provided, the case should in the first instance, be referred to

the management partner, Catherine Thomas who will fully review the details under the Practice’s Complaints Policy & Procedure.

**Related Policies**

Data Protection & Confidentiality Policy

Information Security Policy

Information Governance Policy

**Monitoring & Review**

The Management Partner is responsible for monitoring compliance with this policy and ensuring its effectiveness. This policy will be reviewed every two years, unless a prior review is deemed to be required.

**References**

Access to Health Records Act 1990 c.23

Available at: http://www.legislation.gov.uk/ukpga/1990/23/contents

Access to Medical Records Act 1998 c.28

Available at: http://www.legislation.gov.uk/ukpga/1988/28

Adoption and Children Act 2002 c38

Available at: http://www.legislation.gov.uk/ukpga/2002/38/contents

Children Act 1989 c.41

Available at: http://www.legislation.gov.uk/ukpga/1989/41/contents

Crime and Disorder Act 1998 c.37

Available at: http://www.legislation.gov.uk/ukpga/1998/37/contents

Data Protection Act 1998 c.29

Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents