THAMESMEAD MEDICAL ASSOCIATES

SUBJECT ACCESS REQUEST POLICY

The current DPA 1998 and EU GDPR 2016 (hereinafter called the Data Protection Legislations) details rights of access to both manual data (which is recorded in a filing system) and computer data for the individual/data subject.

This right, commonly referred to as Subject Access Request (SAR) is created under section 7 of DPA 1998 and Article 15 of GDPR 2016, gives rights to a data subject/individual to request personal information Thamesmead Medical Associates holds about them. Anyone with full mental capacity can authorise a representative/third party, for example solicitors/advocates to help them make a SAR.

Under the DPA and GDPR Legislations data subjects have the right to obtain from Thamesmead Medical Associates confirmation as to whether or not personal data concerning the individual/data subject are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure (where necessary) of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority (Information Commission's Office);
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
i) right to be informed about the appropriate safeguards where personal data is transferred to a third country or international organisation;
j) right to request a copy of any personal data undergoing processing.

In line with the Information Commissioner's subject access Codes of Practice, organisations are encouraged to have SAR Policy or Procedure in place to ensure that individuals' rights of access are met within a timely and appropriate manner, and seek to enable all who wish to do so to have access to the records that are held about them.

Aim

This Subject Access Request Policy details how Thamesmead Medical Associates will meet its legal obligations concerning individual's access to their information. The requirements within the Policy are primarily based upon the DPA 1998 and EU GDPR 2016 as they are the key legislations covering rights to personal information.

This Subject Access Request Policy has been written to ensure that all staff of Thamesmead Medical Associates are aware of their responsibilities to provide information if requested.

Patients will also be given a patient information leaflet on Subject Access Requests available at reception or on the practice website www.thamesmedical.org, see appendix 1

Legislations and Code of Practice

For the purpose of this Policy, other relevant legislations and appropriate guidance may be referenced. The legislations listed below refer to issues of security and/or confidentiality of personal data:

- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008
- Information Commissioner's Office: Subject Access Request Code of Practice

Roles and Responsibilities

Accountable Officer

The Data Protection Officer (DPO) Giuseppe Ofori has overall accountability and responsibility for subject access requests. The DPO has delegated SAR operational responsibilities to the Senior Receptionist (Sonia Abbott).

Data Protection Officer

The Data Protection Officer (DPO) has day-to-day responsibilities for the management of all aspects relating to data protection matters. The responsibilities of the DPO include:

- To advise all staff on issues relating to data protection by providing guidance and templates;
- monitor organisational compliance with the Data Protection Legislations including policies and procedures that underpins the protection of personal data within the organisation.
- to provide awareness-raising and training for staff involved in processing operations
- liaise with the Information Commissioner's Officer (ICO) on matters around confidentiality and data protection, information security and records management;
- to provide advice where requested as regards to Data Protection Impact Assessment (DPIA) and monitor the risk management process;
- to consult with the ICO prior to data processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the organisation to mitigate the risk.

The DPO shall in the performance of his functions have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

All Managers and Staff

The Management will ensure that all members of staff are aware of, and adhere to this SAR Policy. They are also responsible for ensuring that the staffs are updated with regards to any changes in the Policy.

All staff has a responsibility to ensure that they comply with the statutory obligations under the Data Protection Legislations, and any guidance lay down to ensure compliance.

Particularly, staff should ensure that:

- They are aware of their responsibility to support SARs and where in the organisation such requests are ultimately handled;
- Personal data and records (whether in electronic or manual) relating to patients/service-users and staff are kept secure, accurate, relevant and up to date.

Staff wishing to access personal confidential information that Thamesmead Medical Associates holds about them should submit their requests in writing.

Thamesmead Medical Associates as a Data Controller

Thamesmead Medical Associates is a data controller in respect of any personal data and special categories of personal within its remit and as part of its statutory functions, Thamesmead Medical Associates determine the purposes for which, and the manner in which those personal information are, or are to be, processed.

Request Process

Patients can make a subject access request in writing or face to face at reception. Patients will also be given a patient information leaflet on Subject Access Requests available at reception or on the practice website www.thamesmedical.org, see appendix 1

If a request is made verbally within a GP/nurse/HCA consultation, then the healthcare professional can, if appropriate and possible within the consultation, provide the requested information immediately as an electronic print off from the computer system. However it is expected that most requests will be formal SAR via reception and outside clinical contacts.

Requirements for a valid subject access request

Adequate steps must be taken to identify the identity of the requester. Each applicant/data subject must be asked to supply one of the following copies of their identification:

- Driving licence
- Passport
- Birth certificate

Notification of Requests

Thamesmead Medical Associates will keep a central register of all requests in order to ensure that requests are cross-referenced with any complaints or incidents and that the deadlines for response are monitored and adhered to. See Appendix 2

Providing personal information under subject access request

SAR provides a right for the data subject/applicant to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, where it is reasonable to do so.

Information must be supplied to the data subject/applicant in an intelligible, easy to understand form, unless to do so would involve 'disproportionate' effort. For manual records this would

involve photocopies. For computerised records these can be supplied as a printout but must contain explanations of codes or abbreviations where appropriate. If the 'disproportionate' effort issue arises, the records can be shared with the individual on a face to face basis who can be asked to visit the premises to view their records.

It is expected that in the majority of cases copies of the relevant record will be give to the patient face to face at reception. It may be possible to post the information to the patient.

If sent by post:

- the record should be sent to a named individual
- by recorded delivery
- marked "private and confidential"
- "for addressee only"
- and the Practice details should be written on the reverse of the envelope.

Use of fax, email and data storage devices is not routinely used.

Types of personal information that can be disclosed

Any information that constitutes personal data or special categories of personal data of the subject/applicant should be provided (subject to any data protection exemptions or information that may cause harm or distress).

Under the Data Protection Legislations the term *"personal data*" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier; they include:

- Demographics - name; address; postcode; telephone number; date of birth;
- an identification number - NHS number, National Insurance Number, location data, an online identifier and Driving licence number [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]

Special categories of personal data include:

- Health records or data concerning a natural person's sex life or sexual orientation
- Genetic data
- Biometrics, DNA Profile, Fingerprints
- Child Protection Records
- Adoption Records
- Tax, Benefit or Pension Records
- Racial or ethnic origin;
- Social Services Records
- Housing Records
- Political opinions;
- Religious or philosophical beliefs

Timescales for responding to subject access requests

Under the EU GDPR Thamesmead Medical Associates is required to respond to subject access requests without undue delay and in any event within **one calendar month** of receipt of the request from the data subject. The period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

In the case of further extension, the DPO or nominated deputy will inform the data subject of any such extension within one calendar month of receipt of the request, together with the reasons for the delay. Failure to do so is a breach of the Legislation and could lead to a complaint being made to the ICO.

To assist the obligation to provide information within the time limits, Thamesmead Medical Associates will ensure that all staff is aware of the SAR process, and requirements to provide the information when requested by the DPO.

Advice and assistance to applicants

Where required, Thamesmead Medical Associates will endeavour to provide advice and assistance in respect to complex request. This may include:

- If the request is unclear and further clarification is needed;
- If the information has been requested in a particular unacceptable, acceptable or unreadable format;
- Where complying with the request would involve disclosure of personal data about another individuals;
- If the information requested is subject to one or more of the exemptions in the Data Protection Legislations.
-

The appropriate limit (Fees)

Request for personal information and communication provided under the GDPR shall be provided free of charge. However, where requests from a data subject are excessive, i.e. requiring extensive resources or administrative time or in particular because of their repetitive character, Thamesmead Medical Associates may either:

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- Refuse to act on the request.

SAR made by a third party/representative of a data subject

Where personal information is being requested by a representative (e.g. solicitor/advocate/next of Kin) of the data subject, Thamesmead Medical Associates must be satisfied that the representative has the authority to make the request on behalf of the data subject and that the appropriate authorisation to act on their behalf has been included.

The representative/third party must be required to provide the following proof of identity of the data subject before personal information can be disclosed:

- Proof of identity i.e. Driving licence or, Passport or birth certificate;
- A signed letter of authorisation from the data subject consenting that the solicitor/advocate can act on their behalf or;
- Lasting Power Attorney (property and financial affairs) or Court of Protection Order if appropriate.

If the Practice (or the individual's GP) thinks an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, we may contact the index patient to discuss further and we may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

Insurance and medical reports do not come under GDRP but Access to Medical Records Act for employment and insurance purposes and these will be chargeable. That is if an insurer/employer

or other organisation is asking for a medical report with interpretation of the data or asking for a medical opinion, this request falls outside the scope of an SAR.

Individuals on behalf of adults who lack capacity

An individual's mental capacity must be judged in relation to the particular decision being made. If a patient has capacity, requests for access by relatives or third parties require his or her consent.

When patients lack mental capacity, health professionals are likely to need to share information with any individual authorised to make proxy decisions such as an individual acting under the authority of a lasting power of attorney.

The Mental Capacity Act in England and Wales contain powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults.

Where there are no nominated individuals, requests for access to information relating to incapacitated adults should be granted if it is in the best interests of the patient. In all cases, only information relevant to the purposes for which it is requested should be provided.

Children

No matter their age, it is *the child* who has the right of access to their information.

Before responding to a subject access request for information held about a child, Thamesmead Medical Associates will consider whether the child is mature enough to understand their rights. If Thamesmead Medical Associates are confident that the child can understand their rights, then we should usually respond directly to the child. **Thamesmead Medical Associates may, however, allow the parent to exercise the child's rights *on their behalf* if the child authorises this, or if it is evident that this is in the best interests of the child.**

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

A person with parental responsibility (see below) may access the records of a competent child if the child consents.

When considering borderline cases, Thamesmead Medical Associates will take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;

- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

Parental responsibility is not necessarily automatic for all parents. A person with

parental responsibility is either:

- the birth mother, or
- the birth father (if married to the mother at the time of child's birth or subsequently)

Unmarried fathers will only have automatic parental responsibility if:

- their child was born after 15 April 2002 (Northern Ireland), 1 December 2003 (England and Wales) or 4 May 2006 (Scotland)

  AND

- the father's name is on the birth certificate

Parental responsibility can also be held by adoptive parents, those appointed as a legal guardian or those given a residence order.

Additionally, when a child is subject to a care order, parental responsibility will be held by the local authority.

Parental responsibility may be acquired or awarded, and it may also be removed by a court order. Parental Responsibility Agreements are another way for fathers, step-parents and registered civil partners to acquire parental responsibility.

Divorce or marital separation does not affect parental responsibility.

When more than one person has parental responsibility, each may independently exercise rights of access.

(This is not an exhaustive list but contains the most common circumstances).

If the appropriate health professional considers that a child patient is Gillick competent (i.e. has sufficient maturity and understanding to make decisions about disclosure of their records) then the child should be asked for his or her consent before disclosure is given to someone with parental responsibility.

Children aged over 16yrs are presumed to be competent.

Children under 16 (in England) must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to an SAR.

If the child is *not* Gillick competent and there is more than one person with parental responsibility, each may independently exercise their right of access.

In all circumstances good practice dictates that a Gillick competent child should be encouraged to involve parents or other legal guardians in any treatment/disclosure decisions.

SAR relating to other individuals who can be identified

Where Thamesmead Medical Associates cannot comply with a request without disclosing information relating to other individuals who can be identified from that information, Thamesmead is not obliged to comply with the request unless –

a) the other individual has consented to the disclosure of the information to the person making the request, or,
b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual, for example, redacting (blanking out) the name or other identifying features.

Where the DPO or nominated deputy establishes another individual's data may be disclosed in an SAR, they will discuss the case with a GP to establish a way forward as above.

Thamesmead Medical Associates will provide the data subjects/applicants with information that constitute their personal information only, and will ensure that a duty of confidentiality owed to the other individual (s) is respected.

Disclosure of information that may harm someone's health

Where a representative/solicitor is making a SAR on behalf of an adult who lacks full mental health capacity, the DPO or staff dealing with the request must be satisfied that the request has been made in the individual's best interest. This may include requesting approval from the data subject's legal guardian or medical practitioner.

A medical professional may believe that providing an individual with access to certain information might cause serious harm to their physical or mental health or to that of another person. If so, the Data Protection (Subject Access Modification) (Health) Order 2000 allows Thamesmead Medical Associates (data controller) to withhold the information. However, only a medical professional can make such a decision, and it must be fully documented.

This exemption does not apply to information the individual already knows.

If an individual disputes some of the information held within their record this should be discussed with the DPO.

Grounds to limit or not provide personal data

There are various grounds where personal data does not have to be provided, in part or in full, these include:

1) Where complying with the request would involve disclosure of personal data about other individuals whom have not given their consent, and redacting (blanking out) their personal information or other identifying features is impossible.
2) Where disclosure would be likely to prejudice an ongoing enquiry or investigation. Where this can be demonstrated Thamesmead Medical Associates do not need to disclose the existence of such information.
3) If the information requested is subject to one or more of the exemptions in the Data Protection Legislations.
4) Where it is a repeated or similar request and Thamesmead Medical Associates had previously complied with the request, unless a reasonable interval has elapsed.
5) If providing documents would involve disproportionate effort or expense. If this is the case the data subject must be informed what information is held, the source of the information, the purpose it is being processed and who it may be disclosed to. This 'exemption' would usually only apply to situations where there is a very large amount of data held within an unstructured (paper) filing system.

   The term 'disproportionate effort' refers to the time and cost of complying with a request and this must be balanced against the effects on the individual requesting the information of not supplying the information. In practice this situation should seldom arise.

Applying an exemption under Data Protection Legislations

The DPA and GDPR give certain provisions which allow public authorities to withhold information from an applicant where an exemption applies. Therefore, in some cases, there will be valid reasons why some information may not be released to an applicant and these include:

- If the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.
- If the disclosure of personal data to third parties contravenes the first data protection principle (process fairly and lawfully).

It is important to note that if an exemption is applied under Data Protection Legislations the DPO or staff of Thamesmead Medical Associates applying the exemption should be aware that they may need to substantiate their decision if challenged by the applicant or the ICO as part of the review process. It is therefore advisable to document decisions (including legal basis) made in relation to using exemption or redaction.

In all cases where an exemption is cited (and a refusal notice issued) the balance of factors for and against should be explained to the applicant in the reply.

Sharing personal data of an individual with law enforcement and regulatory bodies

In some circumstances Thamesmead Medical Associates may be legally required to share personal information with law enforcements and regulatory bodies (without the consent of the data subject). The legal basis and justification for the sharing may be underpinned by the following EU GDPR Articles:

Article 6(C) - sharing/processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 6(e) - the sharing/processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Please see the Thamesmead Medical Associates Privacy note for further information.

Thamesmead Medical Associates will review each request based on its merits before deciding whether to release information to the 'relevant authorities'.

Internal reviews and complaint procedures

If the applicant is dissatisfied with either the way their request has been handled or the response provided, they may make a complaint to the Practice Manager for a review. See TMA complaints policy.

If the applicant remains dissatisfied about the decision, they must be advised on their rights to complain to the Information Commissioner who can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
Tel: 0303 123 1113 or 01625 545 745
Email: https://ico.org.uk/global/contact-us/

Training

Thamesmead Medical Associates will ensure all staff are adequately trained SARs. Training will include but not limited to:

- What information to provide or not to provide
- Correct identification of the requesting individual;
- Location of personal information;
- Timescales for compliance;
- Provision of information in an intelligible format;
- Action to be taken if the information includes third party data

Dissemination and Implementation

This Policy and other related documents will be publicised on Thamesmead Medical Associates website.

Awareness of any new content/change in process will be through the staff communications, in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the DPO.

Monitoring & Compliance

Thamesmead Medical Associates will annually evaluate the effectiveness of this Policy. Quarterly reports will be discussed at our IG monitoring meetings.

Non compliance

Non compliance with this Policy by staff will be brought to the attention of the Practice Manager.

The Data Protection Act gives you the right to see your health records

This is known as the right of access.

A health record is any record of information relating to someone's physical or mental health that has been made by (or on behalf of) a health professional. This could be anything from the notes made by a GP in your local surgery to results of an MRI scan or X-rays.

Health records are extremely personal and sensitive. They can be held electronically or as paper files, and are kept by a range of different health professionals both in the NHS and the private sector.

You do not have to give a reason for applying for access to your health records.

How do I apply to see my records?

If you are registered to EMIS access online, you can access your GP electronic record at any time. Please see reception for further details.

Alternatively you can make an application to access your records via reception (face to face or in writing). As this is sensitive medical information, ID checks will be needed. Someone else, such as a relative or friend can ask for your records for you, but you will need to give your written permission and give proof of ID.

We will give you a print out or photocopy of the relevant information requested. If you have difficulty in understanding the abbreviations or jargon, ask to have these explained to you

We will provide the information within 28 calendar days of your application.

Can I be refused access?

You should also be aware that in certain circumstances your right to see some details in your health records may be limited in your own interest or for other reasons (e.g. to protect the privacy of third parties).

If access is denied or you think information may have been withheld you make a complaint under the NHS complaints procedure or complain to the Information Commissioners Office.

If you have difficulty in understanding the abbreviations or jargon, ask to have these explained to you.

Can I correct the records?

If you think information in your records is inaccurate, you can ask for it to be corrected. If we do not agree to change the record, you can ask that your views are noted for the record. If you are unhappy with the decision you make a complaint under the NHS complaints procedure or complain to the Information Commissioners Office.

What about my children?

No matter their age, it is *the child* who has the right of access to their information. Before responding to a request for information held about a child, it is best practice that we consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should usually respond directly to the child or get their consent before disclosing information to their parents. As a practice we may, however, allow the parent to exercise the child's rights *on their behalf* if the child authorises this, or if it is evident that this is in the best interests of the child.

To apply for access you will need to provide the following:

Adult (16 or over) – Photo ID – Passport or Driving licence – if these are not available a birth certificate can be accepted.

Child – Requesting themselves if component to do so- Photo ID. Passport or driving licence – if these are not available a birth certificate can be accepted.

Child- Someone with Parental responsibility requesting the information - Full birth certificate with parents name on and photo ID of said parent to connect the two.

Third party - carer, next of kin, informal or formal advocate – Signed letter of permission from index patient/Lasting power of attorney/Court of Protection order and Photo ID of index patient. The practice has a right to check with the index patient on information disclosure.

More detailed information on access to your medical information can be found in the Thamesmead Medical Associates Subject Access Request policy available on our website www.thamesmeadmedical.org

Patient's application for subject access request

Patient: Surname.……

Forename: …..……..

Address: ……

……

Telephone number: ……

Date of Birth: ……

NHS No, if known: …….

What records are required? …….

……..

Reason why you need access: …….

Declaration:

I confirm that the information given by me is correct to the best of my knowledge and that I am entitled to apply for subject access request.

- ☐ I am the patient.
- ☐ I have been asked by the patient and attach the patient's written consent and ID.
- ☐ I am a formal advocate for the patient and attach the Lasting power of attorney/court order and ID.
- ☐ I am the patents parent/guardian and the child is under the age of 16.
- ☐ I am the deceased patient's personal representative and attach confirmation of my appointment.

Signed……. Date……

Name……

GRHC to complete:

Application taken by:

Date: