Great Staughton Surgery
Subject Access Request Policy (GDPR Right of Access Policy)

Introduction

Under the General Data Protection Regulation (GDPR), individuals have the right to obtain:

- confirmation that their data is being processed
- access to their personal data (and only theirs)
- other supplementary information – this corresponds to information that should be provided in a privacy notice https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

The GDPR clarifies that the reason for allowing individuals to access their personal data is so they are aware of and can verify the lawfulness of processing and understand how and why the practice is using their data.

An application for access to health records may be made in any of the circumstances explained below. This policy does not apply to requests to access records of deceased patients, as the GDPR does not apply to the data of deceased patients.

Patient Requests

A request for access to health records in accordance with the GDPR can be made in writing to the Practice. A form is available to staff in EMIS for patient requests.

Requests for access can be made verbally or in writing to any member of Practice staff.
All requests will be documented, and the request passed to the Practice Manager (IG lead).
Requests must be recorded in the Subject Access Request register by the staff member receiving the request.

A request does not have to include the phrase “subject access request” or “Article 15 of the GDPR” or “data protection” or “right of access”.

The requester should provide photo identification as proof of their identity (the Practice will verify their identity using “reasonable means”). The Practice must only request information that is necessary to confirm who they are and request photo identity verification when the request is received.

When the requester asks for “a copy of their GP record”, check the information requested is for the *entire* record. The Practice Manager will check with the applicant if full or partial access to information held in the health record is required before processing the request. The GDPR permits the Practice to ask the individual to specify the information the request relates to (Recital 63) where the Practice is processing a large amount of information about the individual. As a result, the information disclosed can be less than the entire GP record by mutual agreement (the individual must agree so voluntarily and freely).

A patient or their representative, is under no obligation to provide a reason for the request, even if asked by the Practice.

Secure Online Records Access

The Practice can offer, if appropriate, for a requester to be enabled to securely access their full GP electronic record online. This would allow them to access all information they might seek. Access should follow identify verification, and a review of the record.

Recital 63 of the GDPR states:
"Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data."

Patients Living Abroad
For former patients living outside of the UK and whom once had treatment for their stay here, under GDPR they have the same rights to apply for access to their UK health records. Such a request should be dealt with as someone making an access request from within the UK.

Patient Representatives
A patient can give written authorisation for a person (for example a solicitor or relative) to make an application on their behalf.

The Practice must be satisfied that the third party making the request *is entitled* to act on behalf of the individual. The third party will provide evident of this entitlement, either written authority or a more general power of attorney (Legal Power of Attorney for Health and Welfare) in the case of an individual who no longer has the mental capacity to manage their own health.

The Practice is entitled to send information requested *directly to the patient* if the patient may not understand what information would be disclosed to a third party who has made a request on their behalf.

A next of kin has no rights of access to medical record, unless they have Power of Attorney.

Court Representatives
A person appointed by the court to manage the affairs of a patient who is incapable of managing their own affairs may make an application. Access may be denied where the GP is of the opinion that the patient underwent relevant examinations or investigations in the expectation that the information would not be disclosed to the applicant.

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, the Practice will consider whether the child is mature enough to understand their rights. If confident that the child can understand, respond directly to the child. The Practice may however, allow a 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 what it means to make a subject access request and how to interpret information they receive.

When considering borderline cases, The Practice should take into account:
- 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 / young person's information. This is important for 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.

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) or,
- an individual given parental responsibility by a court

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

If the appropriate GP considers a child patient is Gillick competent (has sufficient maturity and understanding to make decisions about disclosure of their records) the child should be asked for their consent before disclosure is given to someone with parental responsibility.

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. Technically, if a child lives with, for example, their mother and the father applies for access to the child's records, there is no "obligation" to inform the mother. This may not be practically possible and both parents should be made aware of access requests unless there is a good reason not to do so.

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.

Notification of Requests

The Practice will keep a Subject Access Request Register of all requests in order to ensure that requests and response deadlines are monitored and adhered to. Requests will be created in EMIS and saved into the medical record.

Fees

The Practice must provide a copy of the information **free of charge**. However a reasonable fee can be charged to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.

Manifestly Unfounded or Excessive Requests

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Practice can charge a reasonable fee taking into account administrative costs of providing the information; or refuse to respond.

Where the Practice refuses to respond to a request, the Practice must explain why, informing them of their right to complain to a supervisory authority and to a judicial remedy without undue delay, and at the latest within one month.

Requirement to Consult an Appropriate Health Professional

It is the Practice's responsibility to consider an access request and to disclose the records if the correct procedure has been followed. Before the Practice discloses or provides copies of medical records, records must be checked, and the release must be documented and authorised.

It is the responsibility of the Practice to ensure that the information to be released:

- does not disclose anything that identifies any other data subject. The only exception to this is the identity of people involved in the care of the individual requester, such as community staff or hospital specialists
- does not disclose anything likely to result in harm to the data subject or anyone else
- does not disclose anything subject to a court order or that is privileged or subject to fertilisation or adoption legislation

Grounds for Refusing Disclosure of Health Records

The Practice should refuse to disclose <u>all or part</u> of the health record if the Health Professional is of the view that:

- disclosure would be likely to cause serious harm to the physical or mental health of the patient or any other person; or
- the records refer to another individual who can be identified from that information (apart from a health professional). This is unless
    - that other individual's consent is obtained, or
    - the records can be anonymised, or
    - it is reasonable in all the circumstances to comply with the request without that individual's consent, taking into account any duty of confidentiality owed to the third party

- the request is being made for a child's records by someone with parental responsibility or for an incapacitated person's record by someone with power to manage their affairs, and:
    - the information was given by the patient in the expectation that it would not be disclosed to the person making the request; or
    - the patient has expressly indicated it should not be disclosed to that person

For the avoidance of doubt, the Practice cannot refuse to provide access to personal data about an individual *simply because we obtained that data from a third party.*

Access to Medical Records Act

The Practice will not provide information under a Subject Access Request made on behalf of a patient by a solicitor, insurance agency or employer, and where it is clear that such a request should be made under the Access to Medical Records Act. This refers to reports for employment (proposed or actual) and insurance purposes (any "insurance contract" so covering accident claims, insured negligence, or anything covered by an insurance contract that requires a medical report to support an actual or potential insured claim).

If necessary, the Practice will seek clarification from both the requester and patient concerned.

Informing of the decision not to disclose

If a decision is taken by a GP that the record should not be disclosed, a letter will be sent by recorded delivery to the patient or their representative stating the grounds for refusing disclosure.

The letter must inform the patient or representative without undue delay and within one month of receipt of the request, and will state:

- the reasons you are not taking action;
- their right to make a complaint to the Practice;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

The Practice should also provide this information where a request for a reasonable fee is made, or additional information to identify the individual is required.

Disclosure of the Record

Information must be provided without delay and within one month. This is calculated from the day *after* the request is received, which will be day 1, even if this is a non-working day.

The period for responding to the request begins at receipt of the request, or:

- when the Practice receives any additional information required to confirm the identity of the requester
- when the Practice receives any additional information requested (and required) to clarify the request

Note: In addition to the information requested, the Practice Privacy Notice will also be provided to the individual (filed in: shared / policies & procedures / Info Gov / GDPR guidelines).

When the information is provided by the Practice, this is for personal use only. The security and confidentiality of the records becomes the responsibility of the requestor and the Practice cannot be held responsible for any onward transmission or distribution.

If a request is made verbally, for example within a GP consultation, the GP can - if appropriate and possible within the consultation and, no additional ID verification is required – provide the requested information immediately. Verbal Subject Access Requests should be recorded on the Subject Access Request Register.

The Practice will be able to extend the period of compliance by a further **two months** where requests are complex or numerous. If this is the case, the Practice must inform the individual within **one month** of receipt of the request and explain why the extension is necessary.

Once the appropriate documentation has been received and disclosure approved, the copy of the health record may be prepared, and emailed or handed to the patient or their representative. If the information requested is handed directly to the patient, then verifiable identification must be confirmed at the time of collection.

It should be assumed that if an individual makes a request electronically (i.e. by email), the Practice should provide the information in the same form - electronic format (e.g. as a pdf or word document) and send it to the requester by email.
If sending the information via email, the Practice will

- Check the individual wishes to receive the information by email.
- Check the email address, send a test email and ask for confirmation of receipt, in order to verify the address.
- If in doubt about a recipient email address, the information email should not be sent.
- Test the individual can receive, and access, a test email and attachment via NHSmail's [Secure] encryption service. The individual will need to register to access the information via Trend Micro upon receipt – ask the Practice Manager or IT lead for help.
- Send the information by a secure email from NHSmail, using [Secure] at the start of the subject line, and request the receiver acknowledges receipt.
- Depending on the volume of data to be sent, information may need to be split across multiple [Secure] emails, due to the maximum attachment files size. The individual should be made aware of this where this is the case.

Confidential information will not be sent by email unless:

- the email address of the recipient is absolutely verified and information is sent *securely*
- policy stipulations (unless the patient clearly expresses a preference to receive unencrypted information in this way)

Confidential medical records will <u>not</u> be sent by fax or post.

The following forms are available for staff to complete as appropriate:

- Recording Subject Access Requests made verbally (face-to-face or by telephone)
- Subject Access Request form
- Subject Access Request form where a request is made on behalf of an individual

Review Date	Staff Member	Updated Information
24 May 2018	Practice Manager	