Crown Heights Medical Centre	
RIGHT OF ACCESS POLICY (*Subject Access Request)*	
REVIEW DATE:	**25/10/2021**
REVIEWED BY:	**C Sims DPO**
NEXT REVIEW:	**01/10/2022**

INTRODUCTION

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

The right of access allows individuals to be aware of and verify the lawfulness of the processing,

Under the UK GDPR/DPA 2018, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data (and only theirs)
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (Article 15)

The UK GDPR/DPA 2018 clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63), 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.

The Patient

Crown Heights Medical Centre (hereby referred to as "we" or "the Practice") has a policy of openness with regard to health records and health professionals are encouraged to allow patients to access their health records on an informal basis. This should be recorded in the health record itself.

A request for access to health records in accordance with the UK GDPR/DPA 2018 can be made in writing, which includes by email, to the data controller, i.e. the Practice. A simple form will be provided on our website that patients can use if they wish (and as appended to this policy).

A request for access to health records in accordance with the UK GDPR/DPA 2018 can also be made as a verbal request, especially if the person that the patient is making the request to can verify his/her identity (e.g. their GP). Such a request can be made face-to-face or by telephone, and in such cases a written record of such a request should be documented. That written request should then be passed onto either the Practice Manager or the Information Governance lead.

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 enough proof to satisfy the Practice of their identity (and the Practice is entitled to verify their identity using "reasonable means"). The Practice must only request information that is necessary to confirm who they are.

The default assumption when a requestor asks for "a copy of their GP record" is that the information requested by the individual is the *entire* GP record. However, the Practice may check with the applicant whether all or just some of the information contained in the health record is required before processing the request. The GDPR/DPA 2018 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). This has sometimes been called a "targeted" subject access request.

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 requestor to be enabled to securely access their full GP electronic record online. This would then allow them to access all information that they might be seeking.

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 UK GDPR/DPA 2018 they still 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, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney (LPA 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 the information requested *directly to the patient* if we think that the patient may not understand what information would be disclosed to a third party who has made a request on their behalf.

Court Representatives

A person appointed by the court to manage the affairs of a patient who is incapable of managing his or her 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.

Next of kin

Despite the widespread use of the phrase 'next of kin' this is not defined, nor does it have formal legal status. A next of kin cannot give or withhold their consent to the sharing of information on a patient's behalf. A next of kin has no rights of access to medical records.

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, we should 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. 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.

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.

When considering borderline cases, The Practice should 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.

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 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.

If the child is <u>not</u> 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, its mother and the father applies for access to the child's records, there is no "obligation" to inform the mother. In practical terms, however, this may not be 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 central record 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.

FEES

The Practice must provide a copy of the information **free of charge**.

However, the practice may charge a reasonable fee 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 the administrative costs of providing the information; or
- refuse to respond

Where the Practice refuses to respond to a request, the Practice must explain why to the individual, informing them of their right to complain to the 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 GP'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 the patient's GP must have been consulted and he / she checked the records and authorised the release, or part-release.

It is the responsibility of the GP 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 requestor, such as community staff or hospital specialists
- Does not disclose anything that is 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 TO HEALTH RECORDS

The GP should refuse to disclose all or part of the health record if he / she 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, we cannot refuse to provide access to personal data about an individual *simply because we obtained that data from a third party.*

The rules about third party data apply only to personal data which includes *both* information about the individual who is the subject of the request *and* information about someone else.

Informing of the decision not to disclose

If a decision is taken that the record should not be disclosed, a letter must be sent by recorded delivery to the patient or their representative stating that disclosure would be likely to cause serious harm to the physical or mental health of the patient, or to any other person. The general position is that the Practice should inform the patient if records are to be withheld on the above basis.

If however, the appropriate health professional thinks that telling the patient:

- will effectively amount to divulging that information; or
- is likely to cause serious physical or mental harm to the patient or another individual

then the GP could decide not to inform the patient, in which case an explanatory note should be made in the file.

The decision can only be taken by the GP and an explanatory note should be made in the file. Although there is no right of appeal to such a decision, it is the Practice's policy to give a patient the opportunity to have their case investigated by invoking the complaints procedure. The patient must be informed in writing that every assistance will be offered to them if they wish to do this. In addition, the patient may complain to the Information Commissioner for an independent ruling on whether non-disclosure is proper, and they have the ability to seek to enforce this right through a judicial remedy.

DISCLOSURE OF THE RECORD

Information must be provided without delay and at the latest *within 30 calendar days*. This is calculated from the day *after* the request is received (which will be day 1, and the information must be provided by the end of day 30).

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 requestor

- When the Practice receives any additional information requested (and required) to clarify the request

In addition to the information requested, the additional information that must also be provided (as per Articles 13 and 14) should be included by means of a link to the Practice GDPR Booklet and pointing out the relevant privacy notice (for GP records, this will be "EMIS Health Ltd – EMIS Web").

If a request is made verbally, for example within a GP consultation, then their GP can – if appropriate and possible within the consultation – provide the requested information immediately.

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 the 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 sent to, or given to, the patient or their representative.

There should be no circumstances in which it would not be possible to supply permanent copies of health records.

If the information requested is handed directly to the patient, then verifiable identification must be confirmed at the time of collection.

Confidential information should not be sent by email unless:

- the email address of the recipient is absolutely verified, and
- the information is sent *securely* in line with the Practice "Email and SMS Messaging" policy stipulations (unless the patient clearly expresses a preference to receive unencrypted information in this way)

It should be assumed that if an individual makes a request electronically (i.e. by email), the Practice should provide that information in a commonly used electronic format (e.g. as .pdf or .doc) and provide it to the requestor by email.

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.

The Practice is under no obligation to provide records on USB sticks or CD/DVD ROMS.

At our discretion, however, we may choose to provide the information in this way, but the USB stick or CD/DVD ROM must be new, purchased by the Practice, the data *must* be encrypted, and a charge for the medium can be made.

Copy of Medical Records
Subject Access Request Form (SAR)

General Data Protection Regulation 2018 (GDPR)

***Free online access to your medical records can be obtained via a different form.**

If you would like a copy of the information we hold about you please email our Data Protection Officer nhccg.ch-contact@nhs.net or fill in the form below. We will provide this information free of charge however, we may in some **limited and exceptional** circumstances have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive.

We will provide a paper copy which must be collected by the data subject (patient); we are NOT able to post medical records to you. **Identification will be required when collecting**. Alternatively we are able to send via encrypted email to a verified email address.

Data subject Details

Full Name:
Date of Birth:
Address:
Telephone Number:
Mobile Number:
Email Address:

*Any medical reports emailed are sent via the internet and therefore may not be completely secure, we will send emails encrypted via the NHS Mail system. You will receive instructions of how to open the email.

FOR OFFICE USE	
Date of receipt	
Time of receipt	
Received by	
Patients identity verified	Yes / No
Collection Method	In Person / Email
Pass to Admin	**Date request completed:**
Informed patient ready to collect or Email Yes / No Scan – non workflow.	