DR RYAN & PARTNERS	
ACCESS TO MEDICAL RECORDS POLICY	
Created:	10/05/2018
Created by:	Practice Business Manager
Next review:	1/04/2019

INTRODUCTION

Under the General Data Protection Regulation 2018, patients have the right to apply for access to their health records. Provided that a written application is made by one of the individuals referred to below, Dr Ruddell & Partners (hereby referred to as 'the Practice') is obliged to comply with a request for access subject to certain exceptions (see below). However, the Practice also has a duty to maintain the confidentiality of patient information and to satisfy itself that the applicant is entitled to have access before releasing information.

APPLICATIONS

An application for access to health records may be made in any of the circumstances explained below.

The Patient

A request for access to health records in accordance with the GDPR (the GDPR refers to these as a subject access request) should be made in writing to the data controller, ie. the Practice.

The requester should provide enough proof to satisfy the Practice of their identity and to enable the Practice to locate the information required. If this information is not contained in the original request, the Practice should seek proof as required. Where requests are made on behalf of the individual patient, the Practice should be satisfied that the individual has given consent to the release of their information.

As good practice, 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.

Where an access request has previously been met the GDPR permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between.

A request does not have to use the term 'subject access' or 'data protection' or 'GDPR' for it to be valid.

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

Children of 16 Years or Over

If a mentally competent child is 16 years or over then they are entitled to request or refuse access to their records. If any other individual requests access to these the Practice should first check with the patient that he or she is happy for them to be released.

Children Under 16 Years

Individuals with parental responsibility for an under 16 year old will have a right to access to their medical records. 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 (ie 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 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, 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.

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 may withhold access if it is of the view that the patient authorising the access has not understood the meaning of the authorisation.

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.

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.

Access to a Deceased Patient's Medical Records
Where the patient has died, the patient's personal representative or any person who may have a claim arising out of the patient's death may make an application. Access shall not be given (even to the personal representative) to any part of the record which, in the GP's opinion, would disclose information which is not relevant to any claim which may arise out of the patient's death.

The effect of this is that those requesting a decease person's records should be asked to confirm the nature of the claim which they say they may have arising out of the person's death. If the person requesting the records was not the deceased's spouse or parent (where the deceased was unmarried) and if they were not a dependant of the deceased, it is unlikely that they will have a claim arising out of the death.

Court Children's Services / Family Intervention Team
Where Court Children's Services or the Family Intervention Team has been appointed to write a report to advise a judge in relation to child welfare issues, the Practice would attempt to comply by providing factual information as requested.

Before records are disclosed, the patient or parents consent (where appropriate) should be obtained. If this is not possible, and in the absence of a court order, the Practice will need to balance its duty of confidentiality against the need for disclosure without consent where this is necessary:

- To protect the vital interests of the patient or others, or
- To prevent or detect any unlawful act where disclosure is in the substantial public interest (eg serious crime), and
- Because seeking consent would prejudice those purposes.

The relevant health professional should provide factual information and their response should be forwarded to the designated GP in the Practice for Child Protection who will approve the report.

Amendments to or Deletions from Records
If a patient feels information record on their health record is incorrect then they should firstly make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. If this is unsuccessful then they may pursue a complaint under the NHS Complaints procedure in an attempt to have the information corrected or erased. The patient has a 'right' under the GDPR to request that personal information contained within the medical records is rectified, blocked, erased or destroyed if this has been inaccurately recorded.

He or she may apply to the Information Commissioner but they could also apply for rectification through the courts. The Practice as the data controller should take reasonable steps to ensure that the notes are accurate and if the patient believes these to be inaccurate, that this is noted in the records. Each situation will be decided upon the facts and the Practice will not be taken to have contravened the GDPR if those reasonable steps were taken. In the normal course of events, however, it is most likely that these issues will be resolved amicably.

Further information can be obtained from the Information Commissioner.

PROCESS

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.

Requirement to Consult 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.

Grounds for Refusing Disclosure or Health Records
The GP should refuse to disclose <u>all or part</u> 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 or Practice staff). 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; or

- 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.

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.

Disclosure of a Deceased Patient's Medical Record

The same procedure used for disclosing a living patient's records should be followed when there is a request for access to a deceased patient's records. Access should not be given if:

- The appropriate health professional is of the view that this information is likely to cause serious harm to the physical or mental health of any individual; or
- The records contain information relating to or provided by an individual (other than the patient or a health professional) who could be identified from that information (unless that individual has consented or can be anonymised); or
- The record contains a note made at the request of the patient before his/her death that he/she did not wish access to be given on application. (If while still alive, the patient asks for information about his/her right to restrict access after death, this should be provided together with an opportunity to express this wish in the notes); or
- The holder is of the opinion that the deceased person gave information or underwent investigations with the expectation that the information would not be disclosed to the applicant, or
- The Practice considers that any part of the record is not relevant to any claim arising from the death of the patient.
- The Practice will not process any Access to Records request where the patient's medical records have been returned to Business Services Organisation (BSO).

Disclosure of the Record
Once the appropriate documentation has been received and disclosure approved, a copy of the health record can be 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.

Originals should not be sent.

Confidential medical records should not be sent by fax unless there is absolutely no alternative. If a fax must be sent, it should include the minimum information and names should be removed and telephoned through separately.

All staff should be aware that safe haven procedures apply to the sending of confidential information by fax, for whatever reason. That is, the intended recipient must be alerted to the fact that confidential information is being sent. The recipient then makes a return telephone call to confirm safe and complete receipt. A suitable disclaimer, advising any unintentional recipient to contact the sender and to either send back or destroy the document, must accompany all such faxes. A suitable disclaimer would be:

'Warning: The information in this fax is confidential and may be subject to legal professional privilege. It is intended solely for the attention and use of the named addressee(s). If you are not the intended recipient, please notify the sender immediately. Unless you are the intended recipient or his/her representative you are not authorised to, and must not, read, copy, distribute, use or retain this message or any part of it.'

Confidential Information should not be sent by email unless:

- The email address of the recipient is absolutely verified
- The data is via an encrypted service such as HSC Northern Ireland GP Webmail; or
- The data is fully encrypted via *at least* 128-bit AES and preferably 256-bit AES. In such circumstances, the password must be *at least* 32 characters and contain a mixture of letters (upper and lower case), digits and punctuation. The password must be conveyed to the patient separately from the encrypted file and preferably not by email at all (ie in person, by telephone or post).

If the information is handed directly to the patient then the patient must provide verifiable information at the time of collection.

A note should be made in the file of what has been disclosed to whom and on what grounds.

Where information is not readily intelligible an explanation (eg of abbreviations or medical terminology) must be given and an appointment arranged with the relevant doctor.

Charges and Timescales
Under the GDPR, copies of records should be supplied within one calendar month of receiving a valid and complete access request. In exceptional circumstances, it may take longer.

Where further information is required by the Practice to enable it to identify the record required or validate the request, this must be requested within 14 days of receipt of the application and the timescale for responding begins on receipt of the full information.

Under the GDPR, the Practice will not charge for copies of records. However, a reasonable fee may be applied when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Patients Living Abroad
For former patients living outside of the UK and whom once had treatment for their stay here, under the GDPR 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 a subject access request from within the UK.

Requests made by Telephone
No patient information may be disclosed to members of the public by telephone. However, it is sometimes necessary to give information to another NHS employee over the telephone. Before doing so, the identity of the person requesting the information must be confirmed. This may best be achieved by telephoning the person's official office and asking to be put through to their extension. Requests from patients must be made in writing.

Requests made by the Police
In all cases the Practice can release confidential information if the patient has given his/her consent (preferably in writing) and understands the consequences of making that decision. There is, however, no legal obligation to disclose information to the police unless there is a court order or this is required under statute (eg Road Traffic Act).

The Practices does, however, have a power under the GDPR to release confidential health records without consent for the purposes of the prevention or detection of crime of the apprehension or prosecution of offenders.

The release of the information must be necessary for the administration of justice and is only lawful if this is necessary:

- To protect the patient or another person's vital interests, or
- For the purposes of the prevention or detection of any unlawful act where seeking consent would prejudice those purposes and disclosure is in the substantial public interest (eg where the seriousness of the crime means there is a pressing social need for disclosure).

Only information which is strictly relevant to a specific police investigation should be considered for release and only then if the police investigation would be seriously prejudiced or delayed without it. The police should be asked to provide written reasons why this information is relevant and essential for them to conclude their investigations.

Requests from Solicitors
Solicitors who are acting in civil litigation cases for patients should obtain consent from the patient. The Practice will verify this request with the patient.

Court Proceedings
The Practice may be ordered by a court of law to disclose all or part of the health record if it is relevant to a court case.

FOI and Access to Health Records
The FOI is not intended to allow people to gain access to private sensitive information about themselves or others, such as information held in health records. Those wishing to access personal information about themselves should apply under the GDPR. The Information Commissioner has

provided guidance to the effect that health records of the deceased are exempt from the provisions of FOI due to their sensitive and confidential nature.