Patient Access to Medical Records Policy

Introduction

The Law states that NHS organisations must give a person access to their personal health information, when it is requested. Therefore, a practice must have procedures in place to make access to the information easy and accessible.

There are several areas of legislation that allow the right of the individual to request such personal information are:

- The Access to Medical Reports Act 1988
- The Access to Health Records Act 1990
- The UK General Data Protection Regulation 2021 (UK GDPR)
- The Data Protection Act 2018 (DPA)

Patients requesting their own personal medical records will have their request dealt with under the provisions of the Data Protection Act 2018 and UK GDPR 2021.

Online patient access to services does not change the right that patients must request access to their medical records provided by the provisions of the Data Protection Act (DPA) and UK GDPR. The DPA principles and confidentiality requirements apply in the same way for online access as they do for paper copies of the record.

1. **The Health Record**

   A health record is any record which consists of information relating to the physical and/or mental health or condition of an individual made by a health professional in connection with the care of the individual. It can be recorded in a computerised form, in a manual form or a mixture of both.

   Information covers expression of opinion about individuals as well as fact. Health records may include notes made during consultations and correspondence between health professionals, such as referral and discharge letters, results of tests and their interpretation, X-ray films, photographs, and tissue samples taken for diagnostic purposes. They may also include reports written for third parties, such as insurance companies.

2. **Detailed Patient record Access includes:**

   The minimum specification described by NHS England in the patient online support and resources guide is:

   - Demographic data i.e. name, address, age
   - Allergies and adverse reactions
   - Medication
   - Immunisations
   - Investigation results including numerical values and normal ranges
   - Problems/diagnoses
   - Procedure codes (medical and surgical) and codes in consultations (symptoms and signs)
   - Biological values (e.g. BP)
   - Codes showing referrals made or letters received
   - Other codes (ethnicity, QOF)

   Prospective Detailed Coded Record will also include consultation free text and access to letters.

3. **Medical Records Access – Staff Responsibility**

Practice Manager and Clinical Leads

For the purposes of reviewing requests, the Practice Manager and a named Clinical Lead should ensure current data protection requirements are followed, (the DPO can offer advice and support, if required)

The main duties of these roles are explained below:

Practice Manager or Deputy

- Verify of identity the patient
- Process and co-ordinate the application
- Contact the patient to explain the process
- Review the medical records for third party information and redact information where consent has not been given

Clinical Lead

- Responsibility for reviewing the medical record and limiting or redacting sensitive and/or harmful information.
- Overall responsibility for decision to allow access
- The Clinical Lead will review the content of the medical record and ensure that sensitive or harmful data are not made available to the patient
- The Clinical Lead can refuse the request for the reasons given below
- The Clinical Lead will also check the record for quality, clarity of presentation, completeness, and accuracy.

4. **Requests under the Data Protection Legislation**

The scope of the Data Protection law includes the right of patients to request information on their own medical records. Requests for information under this legislation can be:

- In writing, this includes letter or email
- Verbal requests can be accepted where the individual is unable to put the request in writing or chooses not to. A record of what is requested should be recorded and a letter for approval by the patient sent out (this must be noted on the patient record)
- SARs can also be submitted via social media, such as the practice Facebook page or Twitter
- Be accompanied with appropriate proof of identity (verification documents)

The practice can ask a patient to complete an application form to support the Subject Access Request, although this is not a requirement. Suitably trained and authorised reception staff should ensure the application form has been completed correctly and verify identity. If an application form is used this must be completed and signed by the patient.

Where an information request has been previously fulfilled, the practice does not have to provide the same request again unless a reasonable time-period has elapsed. It is up to the administrative/Clinical Leads to ascertain what constitutes a reasonable time-period.

5. **Detailed Coded Records Access – Application**

Patients will be given a leaflet on the benefits and risks to Detailed Coded Access to Records (promotional links to leaflets can be found below)

On completion of an application form the administrative lead will review the application form and invite the patient into the practice to complete the following:

- Identity Verification
- Inform the patient of the benefits and potential risks to detailed coded access to records
- Advice leaflet will be given to the patient and application process and timescales will be discussed.

The administrative lead will check the records for third party information and redact information where appropriate. If it is not possible to remove information the Clinical Lead should be consulted.

The Clinical Lead will review the content of the medical record and ensure that sensitive or harmful data are not made available to the patient. The Clinical Lead may redact sensitive or harmful data if they consider it to be in the patients' best interest.

The Clinical Lead can refuse the request for the reasons set out below.

The Clinical Lead will also check the record for quality, clarity of presentation, completeness, and accuracy.

If approved, the administrative lead will place an alert on the system to notify other members of staff that the patient has Detailed Coded Record access.

The completed application form should be scanned and attached to the patient's record. The administrative lead will contact the patient to inform them of the outcome of the application, explain the next steps and provide any further information.

6. **Identity Verification**

Access to health records can only be granted when the patient's identity has been verified. There are three ways of confirming patient identity:

- Documentation (Forms of Identification)
- Vouching
- Vouching with confirmation of information held in the applicant's records

All applications for access to health records will require formal identification through 2 forms of ID one of which must contain a photo. Acceptable documents include passports, photo driving licences and bank statements etc.

Where a patient may not have suitable photographic identification – vouching with confirmation of information held in the medical record can be considered. This should take place discreetly and ideally in the context of a planned appointment. It is extremely important that the questions posed do not incidentally disclose confidential information to the applicant before their identity is verified.

Adult proxy access verification - Before the practice provides proxy access to an individual or individuals on behalf of a patient further checks must be taken:

- There must be either the explicit informed consent of the patient, including their preference for the level of access to be given to the proxy, or some other legitimate justification for authorising proxy access without the patient's consent
- The identity of the individual who is asking for proxy access must be verified
- The identity of the person giving consent for proxy access must also be verified. This will normally be the patient but may be someone else acting under a power of attorney or as a Court Appointed Deputy
- When someone is applying for proxy access based on an enduring power of attorney, lasting power of attorney, or as a Court Appointed Deputy, their status should be verified by making an online check of the registers held by the Office of the Public Guardian

Child proxy access verification - Before the practice provides parental proxy access to a child's medical records the following checks must be made:

- The identity of the individual(s) requesting access
- That the identified person is named on the birth certificate of the child
- In the case of a child judged to have capacity to consent, there must be the explicit informed consent of the child, including their preference for the level of access to be given to their parent

Prospective access to patient records online

- In Summer 2022, patients with online access to their medical records will be able to have access to their future full medical records, including free texts, letters, and documents once they have been reviewed and filed by the GP. This will not affect proxy access.
- There will be limited legitimate reasons why access to prospective medical records will not be given or will be reduced and they are based on safeguarding. If the release of information is likely to cause serious harm to the physical or mental health of the patient or another individual, the GP is allowed to refuse or reduce access to prospective records; third party information may also not be disclosed if deemed necessary. On occasion, it may be necessary for a patient to be reviewed before access is granted, if access can be given without a risk of serious harm.

7. **Third Party Information**

A Patients record may contain confidential information that relates to a third person. This may be information from or about another person. It may be entered in the record intentionally or by accident. This does not include information about or provided by a third party that the patient would normally have access to, such as hospital letters.

All confidential third-party information must be removed or redacted. If this is not possible then access to the health records will be refused.

8. **Denial or Limitation of Information**

Access to any health records can be denied or limited. This decision will be made by the Practice Manager and Clinical Lead for the practice.

Access will be denied or limited where, in the reasonable opinion of the Clinical Lead, access to such information would not be in the patient's best interests because it is likely to cause serious harm to:

- The patient's physical or mental health, or
- The physical or mental health of any other person
- The information includes a reference to any third party who has not consented to its disclosure

A reason for denial of information must be recorded in the medical records and where possible an appropriate an appointment will be made with the patient to explain the decision.

When can a subject access request be refused?

The Practice can refuse a request where the request is 'manifestly unfounded or excessive 'or 'repetitive'. The requester must be informed of the reason why within one month of the receipt of the request. If the practice decides to apply this option advice MUST be sought from the practice Data Protection Officer, Tara Moylan at DPO.healthcare@nhs.net or 01270 275217

9. **Timeframe for responding to requests**

The Statutory timeframe has now been reduced to **one month** of receipt of the request, and in any event without delay. In Accordance with Article 12 of the UK GDPR 2021.

This can be extended by a further two months where requests are determined to be 'complex' or 'numerous.

UK GDPR **does not** allow for a fee, so it must be provided free of charge. However, some charges can be made in the following circumstances:

- where further copies are requested by the data subject,
- or the request is manifestly unfounded, or excessive (definitions still required by the ICO) a reasonable fee based on the organisations administration costs may be charged

10. **Proxy Access to Medical Records**

Proxy access is when an individual other than the patient has access to an individual's medical record on their behalf to assist in their care. Proxy access arises in both adults and children and is dealt with differently according to whether the patient has capacity or not.

The patient's proxy should have their own login details to the patient's record. If a patient wants to have more than one proxy, they should all have individual login details. In the current version of our electronic records system (EMIS Web) login details will be shared between the patient and the individual with proxy access.

Proxy access should not be granted where:

- There is a risk to the security of the patient's record by the person being considered for proxy access
- The practice suspects Coercive behavior
- The patient has previously expressed the wish not to grant proxy access to specific individuals should they lose capacity, either permanently or temporarily; this should be recorded in the patient's record
- The Clinical Lead assesses that it is not in the best interests of the patient and/or that there are reasons as detailed in Denial or Limitation of Information

11. **Proxy Access in Adults (including those over 13 years of age) with capacity**

Patients over the age 13 (under UK DPA 2018) are assumed to have mental capacity to consent to proxy access. Where a patient with capacity gives their consent, the application should be dealt with on the same basis as the patient.

In terms of online access, it may be possible to give the proxy different levels of access depending on the wishes of the patient and/or the views of the Clinical Lead, for example, some patients may want to allow a family member to have access only to book appointments and order repeat prescriptions without accessing the detailed care record.

12. **Proxy Access in Adults (including those over 13 years of age) without capacity**

Nursing/residential homes may be granted proxy access for patients under their care.

Proxy access without the consent of the patient may be granted in the following circumstances:

The patient has been assessed as lacking capacity to make a decision on granting proxy access and has registered the applicant as a lasting power of attorney for health and welfare with the Office of the Public Guardian.

The patient has been assessed as lacking capacity to make a decision on granting proxy access, and the applicant is acting as a Court Appointed Deputy on behalf of the patient

The patient has been assessed as lacking capacity to make a decision on granting proxy access, and in accordance with the Mental Capacity Act 2005 code of practice, the Clinical Lead considers it in the patient's best interests to grant access to the applicant.

When an adult patient has been assessed as lacking capacity and access is to be granted to a proxy acting in their best interests, it is the responsibility of the Clinical Lead to ensure that the level of access enabled, or information provided is necessary for the performance of the applicant's duties.

13. **Proxy Access in Children under the age of 11**

All children under the age of 11 are assumed to lack capacity to consent to proxy access. Those with parental responsibility for the child can apply for proxy access to their children's medical records.

Parents will apply for access through the same process outlined in Sections 4 and 5. Additional identification of parental /guardian evidence will be required (see Section 6)

14. **Proxy Access in Children above the age of 11 and under 13 years of age**

Access to medical records will need to be assessed on a case by case basis. Some children aged 11 to 13 have the capacity and understanding required for decision-making with regards to access to their medical records and should therefore be consulted and have their confidence respected

Online proxy access will automatically be turned off when a child reaches the age of 11. Online proxy access to the Detailed Coded Record of children aged 11 to 13 will not normally be approved unless it is in the best interests of the child or is the express wishes of a competent child

The Clinical Lead will invite the child for a confidential consultation to discuss the request for proxy access, whether this is for requests under the Data Protection Law or for online access

The Clinical Lead should use their professional judgement in deciding whether to grant parental access and/or whether to withhold information

If the practice suspects coercive behaviour access will be refused and documented in the medical

notes. The Clinical Lead will liaise with Child Safeguarding teams if appropriate

Online proxy access will also be turned off when a child turns 13. Access can be turned back on by following the processes set out above governing access to adults

15. **Coercion**

Coercion is the act of governing the actions of another by force or by threat, to overwhelm and compel that individual to act against their will.

Online access to records and transactional services provides new opportunities for coercive behaviour.

If the practice suspects coercive behaviour for either an individual or proxy access application, then access will be refused and documented in the medical notes. The Clinical Lead will liaise with CCG Safeguarding Team, if appropriate.

16. **Former NHS Patients Living Outside the UK**

Patients no longer resident in the UK still have the same rights to access their information as those who still reside here and must make their request for information in the same manner.

Original health records should not be given to an individual to take abroad with them, however, the Practice may be prepared to provide a summary of the treatment given whilst resident in the UK.

17. **Staff Training and Education**

All staff at the practice will be required to read the policy and confirm their understanding.

The Data Security e-learning programme has been designed to support staff in health and social care Level 1 – Data security awareness:

This course is mandated for everyone working in health and care. It has been designed to inform, educate and upskill staff in data security and information sharing. It provides an understanding of the principles and importance of data security and information governance. It looks at staff responsibilities when sharing information and includes a section on how to act to reduce the risk of breaches and incidents.

18. **Disputes Concerning Content of Records.**

Once access to medical records has been granted patients often dispute their accuracy or lack understanding of the medical codes that are held in the records.

Patients notice and point out errors in their record these may be unexpected third-party references or entries they object to or want deleted. The right of rectification and deletion are now a right under the UK GDPR.

Reception Staff will pass on any queries to the Practice Manager who will contact the patient and the Practice Manager will investigate to identify the source and extent of the problem.

The Practice Manager will then decide on the most appropriate action. Where the dispute concerns a medical entry the clinician who made the entry should be consulted. Consideration should be given as to whether it is appropriate to change or delete an entry. It is not always possible or practical to contact the clinician who made the entry and in this case the practice Clinical Lead should be consulted. Where a decision is taken not to amend the records an explanation should be given to the patient outlining the reasons why.

If a patient wishes to apply their UK GDPR 2021 rights of

- Rectification (Article 16 UK GDPR)
- Erasure (Article 17 UK GDPR)
- Restriction of Processing (Article 18 UK GDPR)
- Data Portability (Article 20 UK GDPR)

Please contact the practice Data Protection Officer, Tara Moylan at DPO.Healthcare@nhs.net

If the patient further disputes the accuracy once a decision has been made they will be referred to the complaints procedure and/or the Health Ombudsmen.

19. **Complaints**

The practice has procedures in place to enable complaints about access to health records requests to be addressed. Please refer to our practice complaints policy.

All complaints about Access to Records should be referred to the Practice Manager in the first instance or Data Protection Officer, Tara Moylan at DPO.healthcare@nhs.net or 01270 275217

If the patient wishes to make a further complaint, they have the right to do so and should be informed of the NHS complaints procedure.

https://www.gov.uk/government/publications/the-nhs-constitution-for-england/how-do-i-give-feedback-or-make-a-complaint-about-an-nhs-service#how-to-make-a-complaint

or

https://ico.org.uk/make-a-complaint/data-protection-complaints/

or

Sometimes the patient may wish to seek independent Legal advice from a Solicitor

20. **Application Length**

Requests for health records information should be fulfilled within one month (unless under exceptional circumstances – the applicant must be informed where a longer period is required - up to two months extension can be requested – but must be requested from the patient within the first month). Information given should be in a manner that is intelligible to the individual.

Due to the time required to process requests for Detailed Coded Records Access each practice will process applications within 28 working days from date of application. In some circumstances there may be a delay in access to records. Where a longer period is anticipated the patient should be informed.

FAQs

What format should the response be provided in?

Where a request is received by electronic means, unless otherwise stated by the data subject, the information must be provided in a commonly used electronic format.

What are the penalties for non-compliance with the statutory timeframe?

The penalties are still at the discretion of the ICO. However, for non-compliance the financial penalties are now much greater.

What should you do if you identify that you have received a SAR?

Incoming SARs should be passed on immediately to the Practice Manager, where they will be logged, acknowledged, and processed.

If you receive a Subject Access Request, and records are altered with intent to prevent disclosure, this will be committing a criminal offence, and will be punishable by a fine.