

## Patient Access to Medical Records Policy

### Document Control

#### Document Details

Classification:	Good Governance - Information Governance
Author and Role:	Nicole Marshall, Director of Governance
Organisation:	Southport and Formby Health Limited
Document Reference:	09 IG - Patient Access to Medical Records
Initial Version Number:	1.2 - adapted from DPO IG toolkit
Initial Document Approved by:	Board Meeting
Date Approved:	March 2019
Date of first review	March 2020

#### Document Revision History:

Ver	Date	Approved by:	Amendments	Next Review
1.3	June 2020	Governance Committee	Reviewed	June 2021
1.4	May 2021	Governance Committee	Reviewed and dates updated	June 2022
1.5	June 2022	Governance Committee	Brand Update	June 2023

Associated Policies and Resources can be found on  
the GPTN Information Governance Policy page

## 1. Introduction

The Law states that NHS organisations must give a person access to their personal health information when it is requested. Therefore, a company 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 Medical Reports Act 1988
- The Access to Health Records Act 1990
- The General Data Protection Regulation 2016 (GDPR)
- The Data Protection Act 2018 (formerly DPA 1998) (DPA)

Patients requesting their own personal medical records will have their request dealt with under the provisions of the Data Protection Act 2018 and GDPR 2016.

Southport and Formby Health accesses patients' own GP practice records remotely. This policy applies to health records created by clinicians working in our services during consultations, along with any associated correspondence and documents.

## 2. 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.

## 3. 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 (these tend to be held and administered in general practice)
- Investigation results including numerical values and normal ranges
- Problems/diagnoses
- Procedure codes (medical and surgical) and codes in consultations (symptoms and signs)
- Biological values (blood pressure)
- Codes showing referrals made or letters received
- Other codes (ethnicity, QOF)

The Detailed Coded Record can also include consultation free text and access to letters, but this is optional.

## 4. Medical Records Access – Staff Responsibility

### Service Managers and Clinical Leads

For the purposes of reviewing requests, the Service 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:

#### Service Manager

- Verify of identity the patient
- Process and co-ordinate the application
- Contact the patient to explain the process
- Check whether all the individual's health record information is required or just certain aspects
- 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.

## 5. Requests under 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 company Facebook page or Twitter
- Be accompanied with appropriate proof of identity (verification documents)

The company 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 company 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.

### Adult proxy access verification

Before the company 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 company 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

## 6. Third Party Information

A Patient's 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.

## 7. Denial or Limitation of Information

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

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 appointment will be made with the patient to explain the decision.

Can a subject access request be refused?

The Company 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 company decides to apply this option advice MUST be sought from the company Data Protection Officer, Tara Moylan, Howbeck Healthcare at [DPO.healthcare@nhs.net](mailto:DPO.healthcare@nhs.net) or 01270 275217

## 8. 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 GDPR 2016.

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

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 organisation's administration costs may be charged

## 9. 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 company 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

## **10. 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.

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

Nursing/residential homes will not 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.

## **12. 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)

### **13. 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

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

If the company 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

### **14. 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 company 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

### **15. 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 Company may be prepared to provide a summary of the treatment given whilst resident in the UK.

### **16. Staff Training and Education**

All staff at the company 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.

## 17. 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 GDPR.

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

The Service 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 company 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 rights of:

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

Please contact the company Data Protection Officer, Tara Moylan, Howbeck Healthcare at [DPO.Healthcare@nhs.net](mailto: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.

## 18. Complaints

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

All complaints about Access to Records should be referred to the Service Manager in the first instance or Data Protection Officer, Tara Moylan, Howbeck Healthcare on [DPO.healthcare@nhs.net](mailto: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. [Company Complaints policy number 08(a) – available on the GPTN Service Policy page]

[NHS Complaints Procedure](#) or

[ICO - your personal information concerns](#) or

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

## 19. 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 company 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.

### 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. Depending on the severity of the infringement, this could be up to £17m approximately.

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

Incoming SARs should be passed on immediately to the Service 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.

### Additional Support and Documentation that may be of use:

Promotional material for Detailed patient record access:

[GP online services promotional toolkit](#)

[NHS England - Health Publications](#)

### References used:

BMA – Access to Records, General Data Protection Regulations 2016

MDU – Right of Access to Clinical Records, Data Protection Act 2018

NHS England – Patient Online, Access to Health Records 1990

NHS Digital – Records Management Code of Company Health & Social Care Act 2016

NHS Digital – Data Security and Information Governance

NHS England – Identity Verification

ICO – Your Data Matters

ICO – GDPR – Right of Access

ICO – GDPR - Health & Social Care

ICO – GDPR – Children & the GDPR