Access to Medical Records Policy

Document Details	
Title	Access to Medical Records Policy
Main points	Protocol around patients accessing their medical records
Who is the document aimed at?	Clerical teams
Author	
Approval process	
Approved by (Clinician/Manager)	EMT
Most recent approval date	December 2022
Category	Patient
Sub Category	Data Protection
Next review date	January 2024
Distribution	
Who the policy will be distributed to	All staff
Document Links	
Required by CQC	
Other	

Amendments History		
No	Date	Amendment
1	2018	Updated guidance around GDPR/DPA
2	Dec 2021	Added guidance around right to erasure
3	Dec 2022	Added guidance about viewing prospective records on NHS app.
4	July 2023	Updated date of prospective record viewing
5		

Introduction

The law states that NHS organisations must, when requested by an individual, give that person access to their personal health information, and occasionally, certain relevant information pertaining to others. In order to do this, they must have procedures in place that allow for easy retrieval and assimilation of this information. Patients are also (from October 2023) able to see parts of their clinical records through the NHS app without requesting permission.

These are the main areas of legislation that allow the right of the individual to request such personal information, and they are:

- The Data Protection Act 2018 (formerly DPA 1998) (DPA)
- The General Data Protection Regulation 2016 (GDPR)
- The Access to Health Records Act 1990
- The Medical Reports Act 1988

Where the request for information by an individual falls under the legislation of any of these areas, access must be granted.

Patients requesting information about their own personal medical records would usually have their request dealt with under the provisions of the Data Protection Act 2018 and GDPR 2016. There are new requirements regarding Cost and Timeframes for responding to requests, detailed below.

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

A form designed for use by patients and their representatives is contained within the document Guidance for Access to Health Records Requests (DoH February 2010). This is accessible from the link within the Resources section below. See also Access to Medical Record Application form below.

Circumstances around application for access

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

The Patient

Hope Citadel Healthcare 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. The Department of Health's Code of Practice on Openness in the NHS as referred to in HSG (96) 18 Protection and Use of Patient Information will still apply to informal requests.

Such requests are usually made for a reason and will always be in writing. There is no requirement to allow immediate access to a record of any type. The patient may have concerns about treatment that they have received, how they have been dealt with or may be worried that something they have said has been misinterpreted. Staff are encouraged to try to understand and allay any underlying concerns that may have contributed to the request being made and offer an opportunity of early resolution.

Children and Young People

Children over the age of 12 are generally considered to have the capacity to give or withhold consent to release medical records. In Scotland, there is a legal assumption that this is the case, but not in England, Wales, or Northern Ireland where those under 16 should demonstrate that they have the capacity to make these decisions. Where the child is considered to be capable, then their consent must be sought before access is given to a third party. The law regards young people aged 16 or 17 to be adults in respect of their rights to confidentiality.

Access can be refused by the health professional where they consider that the child does not have capacity to give consent / decline decisions.

Individuals with parental responsibility for an under 18-year-old will have a right to request access to those medical records (Scotland under 16). Access may be granted if access is not contrary to the wishes of the competent child. Not all parents have Parental Responsibility.

A person with parental responsibility is either:

a. the birth mother, or
b. the birth father (if married to the mother at the time of child's birth or subsequently) if both are on the birth certificate, or,
c. an individual given parental responsibility by a court.

Parental responsibility is not lost on divorce. If parents have never been married only the mother has automatic parental responsibility, however the father may subsequently "acquire" it.

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 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.

The data controller may refuse access to the record where the information contained in it could cause serious harm to the patient or another person.

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.

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 deceased 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.

Where a deceased patient has indicated that they would not wish disclosure of their records then this should be the case after death unless there is an overriding public interest in disclosing.

Children and Family Court Advisory and Support Service (CAFCASS)

Where CAFCASS has been appointed to write a report to advise a judge in relation to child welfare issues, the practice should attempt to comply by providing factual information as requested.

Before records are disclosed, the patient or parents' consent (as set out above) 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:

1. to protect the vital interests of the patient or others, or
2. to prevent or detect any unlawful act where disclosure is in the substantial public interest (e.g., serious crime), and
3. because seeking consent would prejudice those purposes.

The relevant health professional should provide factual information and their response should be forwarded to a member of the Child Protection Team who will approve the report.

Amendments to or Deletions from Records

If a patient feels information recorded 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 avenue is unsuccessful then they may pursue a complaint under the NHS Complaints procedure to have the information corrected or erased. The patient has a 'right' under the DPA to request that personal information contained within the medical records is rectified, blocked, erased, or destroyed if this has been inaccurately recorded.

They may apply to the Information Commissioner, but they could also apply for rectification through the courts. The GP 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 DPA if those reasonable steps were taken. In the normal course of events, however, it is most likely that these issues will be resolved amicably.

Requirements for Subject Access

Requirements were introduced in 2018 affecting the handling of subject access requests.

As well as providing confirmation that their personal is being processed and providing a copy of this personal data that the data subject has asked for; (subject to any exemptions). Individuals will have the right to be provided with additional information which largely corresponds to the information to be provided in a privacy notice:

- Source of the data.
- Recipient, including details international transfers.
- Retention period for the data.
- How to amend inaccurate data.
- How to complain to the Information Commissioner's Office (internal review will usually need to be satisfied first).

Timeframe for responding to requests

The Statutory timeframe for handing requests is at most one month of receipt of the request, and in any event without delay in Accordance with Article 12 of the GDPR 2016. The period of compliance can be extended by a further two months where requests are determined to be 'complex' or 'numerous'.

The fee of £10-£50 in the previous DPA 1998 has now been removed. It was the case that £10-£50 fee could be charged, but 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
- a reasonable fee based on the organisations administration costs may be charged.

A request may be manifestly unfounded if the person clearly has no intention to exercise their right or if the request is malicious in intent. They may also use the request to harass an organisation, with no real purpose other than to cause disruption. The term 'manifestly' indicates that organisations should provide evidence which demonstrates why the request is unfounded.

Factors that may indicate a manifestly unfounded request include where:

- the person explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated or false accusations against you or specific employees which are clearly prompted by malice;
- the person is targeting a particular employee against whom they have a personal grudge;
- the person makes a request but then offers to withdraw it in return for some sort of benefit from the organisation; or
- the person systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, e.g., once a week.

This is not a simple tick list that automatically means a request is manifestly unfounded.
You **should** consider a request in its own context and consider all the circumstances. The onus is on you to demonstrate that a request is manifestly unfounded.

You **should** consider the particular situation and whether the person genuinely wants to exercise their rights. If they do want to exercise their rights, it is unlikely that the request is manifestly unfounded. In most cases, use of aggressive or abusive language does not, in itself, demonstrate a manifestly unfounded request.

To determine whether a request is manifestly excessive, you **should** consider whether it is clearly or obviously unreasonable. You **should** base this on whether the request is proportionate, when balanced with the burden or costs involved in dealing with the requests.

This means considering all the circumstances of the request, including:

- the nature of the information the request is about;
- the context of the request and the circumstances of the relationship between you and the person;
- whether a refusal to carry out the request or even acknowledge that you hold relevant information may cause substantive damage to the person, such as an adverse impact on their rights. You **should** think about rights broadly by considering any aspect of a person's life;
- your available resources;
- if the request largely repeats previous requests and there has not been a reasonable interval since the last request;
- whether it largely overlaps with other requests (although if it is about a separate set of information, it is unlikely to be excessive); or
- where you have already provided a copy of the information to the person by alternative means.

In most cases, a request is not excessive just because the request covers a large amount of information, even if you find it a burden. As noted above, you **should** consider all the circumstances of the request. If it is a request for access, you **could** also consider asking them for more information to help you locate the information they are looking for.

A repeat request may not be excessive if a reasonable amount of time has passed since their last request. You should consider the following when deciding whether a reasonable amount of time has passed:

- the nature of the data – this could include whether it is particularly sensitive;
- whether the circumstances of the request have changed, for example, can you provide access to information you previously restricted, now that the circumstances have changed?; and
- how often you alter the data.

If it is unlikely that there have been any changes to the information between requests, you **could** decide you do not need to respond to the same request twice.

If you have deleted information since the last request, you **should** let the requester know.

If you have collected new information since their last request then it may not be an excessive request (at least not for the new information).

When can a subject access request be refused?

The Practice can decide to refuse a request where the request is 'manifestly unfounded or excessive', in particular if it is 'repetitive', and 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, Lisa Nolan.

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 at the discretion of the ICO but could be up to £17m in the most extreme cases of data breach. 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.

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

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

When do patients have the right to erasure?

Under GDPR guidance, individuals have the right to request erasure of data held about them. However, this does not automatically relate to health care records, as there is no right to erasure under the following articles:

Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority

Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems

The right to erasure is exempted in a number of healthcare settings and the accepted exceptions include:

1. Medical diagnosis
2. The provision of health or social care
3. The management of health or social care systems or services

This would include warning letters or removal letters held on medical notes as it is relevant to the provision of healthcare and is important in the narrative of care. If patients wish to dispute a removal letter, rather than it being erased, a note can be added on to their medical notes stating that they dispute the letter.

Process

Requests should be in writing, with a patient signature. For the purposes of the DPA email requests are valid, however the practice will need to be satisfied that a valid signature exists prior to disclosure or release. Where a solicitor or other representative is making the request, ensure that you have patient signed consent, and sufficient information to clearly identify the patient.

Notification of requests

Practices should treat all requests as potential claims for negligence. Good working practice would be to 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 checked the records and authorised the release, or part-release.

Grounds for refusing disclosure to health records

The GP should refuse to disclose all or part of the health record if they are 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;
- 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, considering any duty of confidentiality owed to the third party; or if
- 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 this 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.

Non-disclosure of a Deceased Patient's Medical Records

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 their death that they did not wish access to be given on application. (If while still alive, the patient asks for information about their right to restrict access after death, this should be provided together with an opportunity to express this wish in the notes.);
- 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.
- The Practice considers that any part of the record is not relevant to any claim arising from the death of the patient.

Disclosure of the record

Once the appropriate documentation has been received and sufficient identification has been produced to satisfy the data controller that disclosure may be made, then the disclosure may be approved. This can be done either by allowing the patient access to their online record through EMIS patient access, or by sending a copy of the health record to the patient or their representative in a sealed envelope by recorded delivery. If a paper copy is sent, it should be sent to a named individual, marked confidential, for addressee only and the sender's name should be written on the reverse of the envelope. Originals should not be sent. It may be good practice to check with the patient that all of the information requested is, in fact, needed, before fulfilling the request, although there is no requirement under the Act to specify the extent of the requested information as part of the application procedure.

Where viewing is requested, a date may be set for the patient to view by supervised appointment. Where parts of the record are not to be released or to be viewed (i.e., they are restricted) an explanation does not have to be given, however the reasons for withholding should be documented. An explanation of terminology, abbreviation etc must be given if requested. It is good practice for viewings to be supervised by a clinician (e.g., a nurse) who can explain items if needed. Where a non-clinician (e.g., receptionist) does this then no explanation must be offered. Explanation requests should be then referred to a clinical staff member.

Confidential information should not be sent by fax and never by email unless via an encrypted service such as NHS Mail account to another NHS Mail account.

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 (e.g., of abbreviations or medical terminology) must be given.

Where an access request has been fulfilled a subsequent identical or similar request does not have to be again fulfilled unless a "reasonable" time interval has elapsed.

Appropriate Health Professional

The Data Protection (Subject Access Modification) (Health) Order 2000 specifies the appropriate health professional to deal with access matters;

- the current or most recent responsible professional involved in the clinical care of the patient in connection with the information aspects which are the subject of the request, or;

- where there is more than one such professional, the most suitable to advise on the information which is the subject of the request.

Faxes

From April 2020 it is no longer permissible for fax machines to be used within any NHS buildings, which includes doctors' practices in Hope Citadel Healthcare. Therefore, fax must never be used to share medical records with patients or their representatives.

Patients living abroad

For former patients living outside of the UK and whom once had treatment for their stay here, under the DPA 1998 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. Original records should not be given to a patient to take outside the UK. The GP may agree to provide a summary, or otherwise the request is subject to a normal access request under these provisions.

Requests made by telephone

No patient information may be disclosed to members of the public by telephone. However, it is sometimes necessary to give patient 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 their 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 (e.g. Road Traffic Act).

The Practice does, however, have a power under the DPA and Crime Disorder Act to release confidential health records without consent for the purposes of the prevention or detection of crime or 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:

1. to protect the patient or another person's vital interests, or
2. 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 (e.g., 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 using the form that has been agreed with the BMA and the Law Society:

Consent form (England & Wales) bma-access-to-health-records-nov-19.pdf

Court Proceedings

You 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 (for example by a Guardian ad litem).

APPLICATION FOR ACCESS TO MEDICAL RECORDS
Data Protection Act 2018 Subject Access Request

Details of the Record to be Accessed:

Patient Surname	NHS Number
Forename(s)	Address
Date of Birth	

Details of the Person who wishes to access the records, if different to above:

Surname	
Forename(s)	
Address	
Telephone Number	
Relationship to Patient	

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of the Data Protection Act 2018.

Tick whichever of the following statements apply.

- I am the patient.
- I have been asked to act by the patient and attach the patient's written authorisation.
- I am acting in Loco Parentis and the patient is under age sixteen, and is incapable of understanding the request / has consented to me making this request.
  (*delete as appropriate).
- I am the deceased patient's Personal Representative and attach confirmation of my appointment.
- I have a claim arising from the patient's death and wish to access information relevant to my claim on the grounds that…. (please supply your reasons below).

YOUR SIGNATURE.....DATE.....

Continued>>

Details of my Application (please tick as appropriate)

Patient to complete

I am applying for access to view my records only	
I am applying for copies of my medical record	
I have instructed someone else to apply on my behalf	
I have attached the appropriate fee	

Notes:

Under the Data Protection Act 2018 you do not have to give a reason for applying for access to your health records.

Optional - Please use this space below to inform us of certain periods and parts of your health record you may require, or provide more information as requested above.

This may include specific dates, consultant name and location, and parts of the records you require e.g. written diagnosis and reports. Note: defining the specific records you need may result in lower fee charges and a quicker response.

I would like a copy of all records	
I would like a copy of records between specific dates only (please give date range) below	

I would like copy records relating to a specific condition / specific incident only (please detail below)	