Access to Medical Records Policy

Introduction

Policy statement

The law states that organisations must, when requested by an individual, give that person access to their personal health information and, occasionally, certain relevant information pertaining to others. To do this, they must have procedures in place that allow for the easy retrieval and assimilation of this information.

The purpose of this document is to ensure appropriate procedures are in place at The Lakeside Practice to enable individuals to apply for access to health records (commonly referred to as a medical record), whether online or by requesting a copy, and to enable authorised individuals to apply for access to information held about other people by making a subject access request (SAR).

This is particularly relevant to the administration and reception staff; however, all staff should be aware of the available online services and SAR process and be able to advise patients, relatives and carers of the appropriate process.

Failure to comply with the policy and any associated breaches of patient data or confidentiality could lead to prosecution or imposition of penalties by the Information Commissioner's Office (ICO).

Access to medical records can be provided via:

- An online portal linked to the organisation's webpage
- A variety of NHS approved apps
- A verbal SAR
- A written SAR including email and/or through social media

This policy is written in conjunction with the following government legislation:

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data Protection (Subject Access Modification) (Health) Order 2000
- Mental Capacity Act 2005

Throughout this document, references have been taken directly from the ICO.

Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.
This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your

contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

Definition of terms

Personal identifiable data (PID)

The ICO states that this is information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier.

The UK General Data Protection Regulation (GDPR) definition provides for a wide range of personal identifiers to constitute personal data including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Prospective access

Future (prospective) records access means access to information and data added to the patient record from a set date onwards. This may be the date that a patient joined the practice or from a date when access has previously been granted.

Patients are being given online account access to their future, or prospective, full general practice health record including free text, letters and documents. Patients will see new information once it is entered or filed onto their record in the clinical system. Patients will not see their historic or past health record information unless they have already been given access to it by their general practice

NHS Digital provides full guidance here.

Proxy access

Proxy access refers to access to online services by somebody acting on behalf of the patient and usually with the patient's consent, by somebody other than the patient for example the patient's parent or carer.

Details for when proxy access might be enabled can be found in this RCGP guidance document.

Lasting power of attorney

A lasting power of attorney (LPA) is a legal document that lets the patient appoint one or more people (known as 'attorneys') to either to help make any decisions or to make any decision on the persons behalf.

For further information about this including how to make, register or end an LPA, see here.

Responsible clinician

The responsible clinician is the most appropriate health professional to deal with the access request who is the current or more recent responsible professional involved in the clinical care of the patient in connection with the aspects of information that are the subject of the request. When there is more than one such professional, the most suitable should advise.

Sensitive personal data

The UK GDPR refers to sensitive personal data as "special categories of personal data".

The special categories specifically include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data (when processed to uniquely identify an individual), data concerning health or data covering an individual's sex life or sexual orientation.

Personal data relating to criminal convictions and offences is not included but similar extra safeguards apply to its processing.

Right to access

This organisation ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

- Waiting room
- Organisation website
- Organisation information leaflet

To comply with the UK GDPR, all organisation privacy notices are written in a language that is understandable to all patients and meets the criteria detailed in Articles 12, 13 and 14 of the UK GDPR. There are privacy notices for both the Practice and Children.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

Detailed information about access for third parties can be found at Chapter 10.

Patient access to online medical records

Background

Patient Online was designed to support GP organisations offering and promoting an online service to their patient population. The service is referred to as GP online services and is offered to patients in addition to telephone and face-to-face interactions at GP organisations.

As of 31 October 2023, all patients should have been granted online access to their full record, including the ability to add their own information, with new registrants of an organisation having full online access to the digital record for their prospective information starting from the date of their registration for online services.

The NHS Digital document titled Online access to GP health records details how patients with online accounts such as the NHS App will be able to read new entries, including free text, in their health record. This change only applies to future (prospective) record entries and not historic data.

The following links provide supporting information to enable understanding and implementation:

- RCGP GP Online Services toolkit
- NHS Digital
  - Videos to explain key topics
  - Learning from the early adopter sites
  - Essential communication materials and practice readiness checklist for general practice to use to inform their patients and to ensure practices can confidently complete a range of necessary actions that includes staff training and a review of relevant policies and processes
- NHS England Practice guidance Offering patients prospective record access

The organisation will need to be mindful that this level of access will be the default for all patients within the clinical system. It is therefore imperative that organisations know how to manage their workflows ensuring sensitive information is redacted as it is entered onto the clinical system or, in rare circumstances, know when it may be inappropriate to give a patient access to their record. Patients will see new information once it is entered or filed onto their record in the clinical system.

In addition to the detailed coded record, access to a full patient record includes free text consultation notes and documents, i.e., hospital discharge letters, referral letters etc.

Registering for online services

At this organisation, staff are to remind patients that GP online services are free and available to all registered patients. NHS England has published a number of guides and leaflets that provide further detailed information about how patients can access their health record online.

Patients who wish to register for online services to book or cancel appointments, order repeat prescriptions and view their medical records and clinical correspondence online are to complete the registration form at Annex A. Note that this will be for retrospective access as prospective information moving forward will already be available.

Additionally, those applicants wishing to apply for access to retrospective information held about other people must complete the appropriate sections on the registration form also at Annex A and the application should be processed in line with the requirements outlined in the proxy access and third-party requests section.

For those patients unable to visit their own GP organisation, NHS Digital provides access to sign up for online services here where there is a requirement to provide appropriate identification using a mobile phone as part of the process.

Prospective access to full records is subject to the same safeguarding information requirements as applied to DCR access. Requests for access can be refused and further detail is provided in the refusal to comply with a request and coercion sections.

Unlike registration, ID verification is required to ensure that online access is granted only to the patient or their authorised representative(s). All patients will be requested to provide two forms of ID verification in line with NHS England's Good Practice Guidance on Identity Verification and the organisation accepts appropriate forms of ID outlined in the identity verification section.

Completed documentation will be reviewed by the responsible clinician for processing including the review of the online records for third party references and any information that may cause harm or distress to the patient/applicant that may need to be hidden from online access using confidentiality policies (see Third party information and Non-disclosure sections).

For all applications, requesters should be advised that it will often take several days to process any online service request.

Post-registration

Once a patient has registered at the organisation and the request has been processed, they are to be issued with a letter that includes their unique username, password and instructions on how to access the online services.

Only the completed registration form should be scanned into the individual's healthcare record.

Guidance documentation

Further detailed guidance in relation to registering patients for online services can be found here.

Summary Care Records (SCR)

About

Summary Care Records (SCR) are an electronic record of important patient information created from GP medical records. They can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care.

Access to SCR information means that care in other settings is safer, reducing the risk of prescribing errors. It also helps to avoid delays to urgent care. At a minimum, the SCR holds important information about:

- Current medication
- Allergies and details of any previous bad reactions to medicines
- The name, address, date of birth and NHS number of the patient

Further reading can be sought from NHS Digital's Summary Care Records.

Additional information in the SCR, such as details of long-term conditions, significant medical history or specific communications needs, is now included by default for patients with an SCR unless they have previously told the NHS that they do not want this information to be shared.

Should a patient not wish to have any additional information shared, they can complete the SCR patient consent preference form.

Further reading can be sought from NHS Digital's Additional information on the SCR and a patient information for additional or enhanced summary care records can be found in this poster.

National Care Records Service (NCRS)

The platform to authenticate SCR applications (SCRa) is a legacy system and has been switched over to the National Care Records Service (NCRS).

Further information including guidance on what is needed to be undertaken and the benefits of having NCRS can be found at the NHS Digital webpage titled Switching over from SCRa to NCRS.

COVID-19 and SCR

To help the NHS to respond to the coronavirus (COVID-19) pandemic, there is currently a temporary change to the SCR that includes COVID-19 specific codes in relation to the suspected, confirmed, shielded patient list and other COVID-19 related information. This information is also retained in the additional information.

Further reading can be sought from NHS Digital's document titled Summary Care Records - Information for Patients.

Third-party requests for medical information

About

Many requests for medical information would be via a SAR and these would ordinarily be received by either the patient or their representative, or from a solicitor or insurer.

However, requests for medical information can also be received by other means, such as private healthcare providers. In these instances the request would not necessarily be received via a SAR, instead it may simply be a letter that includes the patient's consent to release the required information.
To promote safer data protection working practices, upon receipt of any request and even with a signed consent form, this organisation will contact the subject (patient) to confirm that this request is bona fide.

Subject Access Requests (SAR) to medical records

In accordance with Article 15 of the UK GDPR, individuals have the right to access their data and any supplementary information held by this organisation. Further detailed information is available in the UK GDPR Policy.

SARs are predominantly used for access to, and the provision of, copies of medical records. This type of request need not always be in writing (e.g., letter, e-mail). However, applicants

should be offered the use of a SAR application form which allows for the explicit indication of the required information.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

When a data subject (individual) wishes to access their data, they are to be encouraged to use the SAR form which can be found at Annex B. All staff must note that the ICO states, *"An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data".*

Furthermore, SARs can be submitted online or via social media as detailed within the NHS webpage titled How to get your medical records. Any requests not using the SAR form will still be processed.

To request a SAR, the requester must be:

- The data subject OR
- Have the written permission of the data subject OR
- Have legal responsibility for managing the subject's affairs to access personal information about that person, such as a lasting power of attorney (LPA)

It is the requester's responsibility to satisfy this organisation of their legal authority to act on behalf of the data subject. The organisation must be satisfied of the identity of the requester before they can provide any personal information (see Identity verification section).

Requests may be received from the following:

- **Competent patients**

  May apply for access to their own records or authorise third party access to their records.

- **Children and young people**

  May also apply in the same manner as other competent patients. This organisation will not automatically presume a child or young person has capacity under the age of 16. However, those aged 13 or over are expected to have the capacity to consent to medical information being disclosed.

  Note the BMA guidance titled Access to health records states the age is 12, although it is 13 with UK GDPR and also that age in the CQC GP Mythbuster 8: Gillick competency and Fraser guidelines.

- **Parents**

  May apply to access their child's health record providing this is not in contradiction of the wishes of the competent child.

  Further guidance on parental access to a child's healthcare records is detailed within the BMA guidance titled Children and young people ethics toolkit and at Section 10.4.

- **Individuals with a responsibility for adults who lack capacity**

  Are not automatically entitled to access the individual's health records. This organisation will ensure that the patient's capacity is judged in relation to the particular decisions being made.

  Any consideration to nominate an authorised individual to make proxy decisions for an individual who lacks capacity will comply with the Mental Capacity Act 2005 in England and Wales and the Adults with Incapacity Act in Scotland.

- **Next of kin**

  Have no rights of access to health records.

- **Police**

  In all cases, the organisation 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 statutes (e.g., Road Traffic Act 2006).

  Nevertheless, health professionals have a power under the Data Protection Act 2018 and the Crime Disorder Act 1998 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:

    - 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 (e.g., when the seriousness of the crime means there is a pressing social need for disclosure)

  Only information that 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.

- **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 when the responsible clinician 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.

- **Patient representatives/solicitors**

  A patient can give written authorisation for a person (for example a solicitor or relative) to make an application on their behalf for copies of their medical records.

This organisation may withhold access if it is of the view that the patient authorising the access has not understood the meaning of the authorisation. It is important to stress to the patient that under a SAR, all health records are provided unless a specific time period is stated and patients should be mindful of giving access to this level of health data.

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. If a consent form from the patient is not received with the application form then no information must be provided until this has been received.

- **Requests for insurance medical reports**

  SARs are not appropriate should an insurance company require health data to assess a claim. The correct process for this at this organisation is for the insurer to use the Access to Medical Reports Act 1988 when requesting a GP report.

  In most cases, the requester will provide the patient's signed consent to release information held in their health record. The BMA have issued guidance on requests for medical information from insurers.

  Therefore, this organisation will contact the patient to explain the extent of disclosure sought by the third party. The organisation can then provide the patient with the medical record as opposed to the insurer. The patient is then given the opportunity to review their record and decide whether they are content to share the information with the insurance company.

  Insurers are to be advised that the following fees are applicable and as detailed within BMA Guidance Fees:

  - GP report for insurance applicants £104.00
  - GP supplementary report £27.00

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures. The use of the organisation's SAR form supports the data controller in verifying the request. In addition, the data controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e., driving licence or passport.

Further reading can be sought from the BMA's Access to health records guidance.

Processing a SAR request

Upon receipt of a SAR, a record of this is to be detailed within the health record of the individual to whom it relates, as well as annotating the Data Subject Access Request (SAR) Register. Further to this, once processed, another entry onto the health record should be made, including the date of postage or the date the record was collected by the patient or authorised individual in addition to updating the SAR Register.

Under the Data Protection (Subject Access Modification) (Health) Order 2000, an appropriate healthcare professional (responsible clinician) manages all access matters. Whenever possible, the healthcare professional most recently involved in the care of the patient will review and deal with the request. If, for some reason, they are unable to manage the request, an appropriate professional will assume responsibility and manage the access request.

To maintain UK GDPR compliance, the data controller will ensure that data is processed in accordance with Article 5 of the UK GDPR and will be able to demonstrate compliance with the regulation (see the organisation's UK GDPR Policy for detailed information).

Data processors will ensure that the processing of personal data is lawful and at least one of the following applies:

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary to protect the vital interests of the data subject or another natural person

Individuals will have to verify their identity. It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures. Further information can be sought from the NHS England document titled Good practice guidance on identity verification and the Identity verification section.

The process upon receipt of a SAR form is illustrated at Annex E which is an aide-memoire/flow diagram for staff. A poster explaining how to access health records for use in waiting room areas can be found at Annex F.

Timeframe for responding to requests

In accordance with the UK GDPR, patients are entitled to receive a response within the maximum given time frame of one calendar month from the date of submission of the SAR.

To ensure full compliance regarding SARs, this organisation will adhere to the guidance provided in the UK GDPR. In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the applicant must be informed in the first month and the reasons for the extension given.

Should the request involve a large amount of information, the data controller will ask the data subject to specify what data they require before responding to the request. Data controllers are permitted to 'stop the clock' in relation to the response time until clarification is received.

Further reading can be found in the BMA document titled Access to health records.

Fees

With regard to the UK GDPR, SARs are generally free of charge. Only if the SAR is 'manifestly unfounded' or 'excessive' can a 'reasonable' fee be charged although the circumstances when a fee can be charged are rare and should be on a case-by-case basis.

The ICO has advised that a request could be deemed as ‘excessive’ if an individual was to receive information via a SAR and then request a copy of the same information within a short period of time. In this scenario, the organisation could charge a reasonable fee or refuse the request. Postage costs for SARs should not be charged for unless they are 'unfounded or excessive'.

Further reading can be found in the BMA document titled Access to health records.

Method of response to requests

The decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided.

Should an individual submit a SAR electronically, this organisation will reply in the same format (unless the data subject states otherwise).

When the patient/applicant requests their information to be emailed to them, it is strongly recommended that the organisation explains to the patient/applicant the risks (for example, unauthorised interception of the data) of receiving the data via unencrypted means to a non-NHS email address. The organisation should document the patient’s agreement (expressed in writing or via email) to receive their data via unencrypted means in the medical record. If the patient/applicant agrees, a USB stick or a CD can be used as alternative electronic formats.

For those requests that are not made electronically, a paper copy can be provided unless the patient has explicitly requested a different format.

Amendments to medical records

Records should not be amended because of a request for access. Indeed, it is a criminal offence under the Data Protection Act 2018 to amend or delete records in response to a SAR. If amendments are made between the time that the request for access was received and the time at which the records were supplied, these must only be amendments that would have been made whether or not the request for access was made. When dealing with a SAR, the most up to date information should be provided.

Information that is clinically relevant must not be deleted from medical records (for electronic records, information can be removed from display but the audit trail will always keep the record complete). Amendments to records can be made provided the amendments are made in a way that indicates why the alteration was made so that it is clear that records have not been tampered with for any underhand reason.

Patients may also seek correction of information that they believe is inaccurate (see the Disputes concerning content of records section).

iGPR

When a request is received via iGPR, it should be processed in accordance with the organisation’s iGPR protocol. iGPR will automatically find and redact items in a record that should not be included. To ensure all relevant attachments are included in the report

(including any hard copies that are not within the patient's electronic healthcare record), the report should not be processed on iGPR until it is certain that the entire record has been scanned into the patient's record within the clinical record system.

Once this has been confirmed, the request can be processed but the staff member processing the request must then assign the report to the responsible clinician who will review this and confirm accuracy before agreeing it can be sent using iGPR.

Further information, including training videos and infographics for iGPR, can be sought here.

Additional Privacy Information notice

Once the relevant information has been processed and is ready for issue to the patient, it is a requirement, in accordance with Article 15 of (UK GDPR), to provide an Additional Privacy Information notice (APIn), the template for which can be found at Annex G.

Organisation disclaimer

The template at Annex H is to be used when issuing patients with copies of their medical records. This outlines the fact that the patient is responsible for the security and confidentiality of their records once they leave the organisation and that the organisation will not accept any responsibility for copies of medical records once they leave the premises.

Refusal to comply with a request

This organisation will only refuse to comply with a SAR when exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the data controller will inform the individual of:

- The reasons why the SAR was refused
- Their right to submit a complaint to the ICO
- Their ability to seek enforcement of this right through the courts

Each request must be given careful consideration and, should it be refused, this must be recorded and the reasons for refusal justifiable.

Being the data controller, the ICO details that an organisation has the right to refuse any online access or SAR although any such refusal will be within the allotted timescale and the reasons for the refusal will be given.

A letter template for refusal can be found at Annex I.

There are occasions when a healthcare professional may firmly believe that it is not appropriate to share all the information contained in the individual's record, particularly if there is potential for such information to cause harm or distress to individuals or when the record contains information relating to a third party. This information can be redacted from the patient's view but must not be deleted from the record (see non-disclosure section). If system functionality to redact information is not available, the record should not be shared with the patient.

Further reading can be sought from the GMC document titled When you can disclose personal information.

Coercion

The risks of coercion of patients with online access should always be borne in mind. Patients may be forced into sharing information from their record including log-in details, medical history, repeat prescription orders, appointment booking details and other private, personal information. By gaining access to a person's record, an abuser may gain further control or escalate harm.

Registering patients for online services requires awareness of the potential impact of coercion and children, adults in an abusive relationship and the elderly or otherwise vulnerable adults can all be victims. Access to a patient's health record can be particularly attractive to an abusive partner, carer or parent.

All staff involved in registering patients for online services are aware of the potential impact of coercion and the signs to look out for to help patients who might be subject to coercion.

Further reading on coercion can be sought within The Safeguarding Handbook and the Home Office webpage titled Domestic abuse: how to get help can provide guidance on actions that can be taken should coercion be suspected.

Non-disclosure

The UK GDPR provides for several exemptions in respect of information falling within the scope of a SAR. In summary, information can generally be treated as exempt from disclosure and should not be disclosed, if:

- It is likely to cause serious physical or mental harm to the patient or another person
- It relates to a third party who has not given consent for disclosure (when that third party is not a health professional who has cared for the patient) and after considering the balance between the duty of confidentiality to the third party and the right of access of the applicant, the data controller concludes it is reasonable to withhold third party information
- It is requested by a third party and the patient had asked that the information be kept confidential or the records are subject to legal professional privilege, or, in Scotland, the records are subject to confidentiality as between client and professional legal advisor. This may arise in the case of an independent medical report written for the purpose of litigation. In such cases, the information will be exempt if, after considering the third party's right to access and the patient's right to confidentiality, the data controller reasonably concludes that confidentiality should prevail or it is restricted by order of the courts
- It relates to the keeping or using of gametes or embryos or pertains to an individual being born because of in vitro fertilisation
- In the case of children's records, disclosure is prohibited by law, e.g., adoption records

The data controller must redact or block out any exempt information. Depending on the circumstances, it may be that the data controller should take steps to explain to the applicant how the relevant exemption has been applied. However, such steps should not be taken if, and insofar as they would, in effect cut across the protection afforded by the exemptions. Indeed, in some cases even confirming the fact that a particular exemption has been applied may itself be unduly revelatory (e.g., because it reveals the fact that the information sought is held when this revelation is itself is unduly invasive of relevant third-party data privacy rights). There is still an obligation to disclose the remainder of the records.

While the responsibility for the decision as to whether to disclose information rests with the data controller, advice about serious harm must be taken by the data controller from the responsible clinician. If the data controller is not the responsible clinician, then the appropriate responsible clinician needs to be consulted before the records are disclosed. This is usually the healthcare professional currently or most recently responsible for the clinical care of the patient in respect of the matters that are the subject of the request. If there is more than one, it should be the person most suitable to advise. If there is none, advice should be sought from another healthcare professional who has suitable qualifications and experience.

Circumstances in which information may be withheld on the grounds of serious harm are extremely rare and this exemption does not justify withholding comments in the records because patients may find them upsetting. When there is any doubt as to whether disclosure would cause serious harm, the BMA recommends that the responsible clinician discusses the matter anonymously with an experienced colleague, their Data Protection Officer (DPO), the Caldicott Guardian or a defence body.

Proxy access

Proxy access to medical records

Some patients find it helpful for a second person to have access to their online GP record. This is often a family member, medical next of kin, a close friend or a carer whom they trust to act on their behalf. The patient can, however, limit which online services they want the nominated individual to access.

This is called proxy access and arises in both adults and children and is dealt with differently according to whether the patient has capacity or not.

Proxy access should not be granted where:

- The organisation suspects coercive behaviour (See Coercion chapter)
- There is a risk to the security of the patient's record by the person being considered for proxy access
- 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 responsible clinician 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

The arrangement for proxy access may be formal or informal and this is detailed in the NHS England document titled Proxy Access. Further reading on this subject can be found in the NHS Digital document titled Linked profiles and proxy access.

A more formal approach can be to delegate a lasting power of attorney (LPA). Further information about LPA scan be sought from Chapter 11.

Proxy access in adults with capacity

Under the Data Protection Act 2018, patients over the age of 13 are assumed to have mental capacity to consent to proxy access. When a patient with capacity gives their consent, the application should be dealt with on the same basis as the patient. Annex C is a consent form to allow nominated persons with capacity access to specific areas of a named person's medical records.

This form can be used for a named proxy to simply book an appointment or order medication, or for greater access such as to have access to obtaining test results or consultations. The form has tick boxes that specifically allow a named person to have partial or full access to the named person's healthcare information. This form must be signed by the patient prior to being considered valid. Any concerns with regard to coercion must be discussed with the safeguarding lead.

It should be noted that this form does not permit any third party individual to make healthcare decisions on behalf of the named patient. Furthermore, the patient is responsible for this agreement and any changes or updates that may be required at a later date.

Chapter 12 details the requirement to confirm any third party's identity.

For children and young people refer to Section 10.4.

Proxy access in adults without capacity

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

- The patient has been assessed as lacking capacity to decide 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 decide 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 responsible clinician 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 responsible clinician to ensure that the level of access enabled, or information provided is necessary for the performance of the applicant's duties

Annex D provides a template to support these requests.

Children and young people's access

It is difficult to say at what age the child will become competent to make autonomous decisions regarding their healthcare as between the ages of 11 and 16 this varies from person to person. In accordance with Article 8 of the UK GDPR, from the age of 13 young people can provide their own consent and will be able to register for online services.

It should be noted that the age is deemed to be 12 years in the BMA document Access to health records although this should always be assessed by the clinician as to whether they are deemed competent. The CQC's GP Mythbuster 8: Gillick competency and Fraser guidelines advises that while there is no lower age limit, it would rarely be appropriate for a child under the age of 13 to consent to treatment.

For detailed guidance for children, the RCGP has raised a document titled Children and Young People which explores proxy access and how the child's 11th and 16th birthdays act as specific milestones.

Proxy access without consent

The organisation may authorise proxy access without the patient's consent when:

- The patient does not have capacity to make a decision on giving proxy access
- The applicant has a lasting power of attorney (health and welfare)
- The applicant is acting as a Court Appointed Deputy on behalf of the patient
- The GP considers it to be in the patient's best interests

The person authorising access has responsibility to ensure that the level of access enabled is appropriate for the performance of the applicant's duties.

The nominated individual is to complete the online services registration form at Annex A or the SAR application form at Annex B. Should the organisation opt not to grant the person access to an individual's record, the responsible clinician will contact the patient and advise them of the reasons why this decision has been reached.

The organisation may refuse or withdraw formal proxy access at any time if they judge that it is in the patient's best interests to do so. Formal proxy access may be restricted to less access than the patient has, e.g., appointments and repeat prescriptions only.

Patients who choose to share their account credentials with family, friends and carers (including a care home) must be advised of the risks associated with doing so. Formal proxy access is the recommended alternative in all circumstances.

Further information on competency for children and young people can be sought in the Consent Policy.

Parents gaining access to a child's medical record

This organisation will allow parents access to their child's medical records if the child or young person consents or lacks capacity and it does not go against the child's best interests.

However, if the records contain information given by the child or young person in confidence then this information should not normally be disclosed without their consent.

It should be noted that divorce or separation does not affect parental responsibility and therefore both parents will continue to have reasonable access to their children's health records unless legally advised not to do so.

Further reading on this subject can be sought in the GMC document titled Accessing medical records by children, young people and parents. Likewise, there are sections on both separated parents and parental responsibility within The Safeguarding Handbook.

Lasting power of attorney

About

A lasting power of attorney (LPA) is a legal document that allows individuals to give people they trust the authority to manage their affairs if they lack capacity to make certain decisions for themselves in the future.

To nominate an LPA, the person must be over 18 years old and have the ability to make their own decision (mental capacity). There are two types of LPA, the vast majority of LPAs deal with health and welfare although occasionally there may be a need to be involved with LPAs that property and financial affairs.

For further information about this including how to make, register or end an LPA, see here.

Responding to an access request

When someone is applying for proxy access on the basis of an enduring power of attorney, an LPA 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 here.

Should an LPA have been granted, this will allow the nominee to access healthcare records for the patient that they are acting on behalf of. This may include sharing medical records with other third parties as they deem appropriate.

An example could be when a patient without capacity is in a care home. A template for this can be found at Annex D.

Should there be any concern about an LPA, then Government advice can be found here.

Identity verification

Requirement

Before access to health records is granted, the patient's identity and the requestor's identity in cases of proxy access requests must be 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 will require formal identification through two forms of ID, one of which must contain a photo. Acceptable documents include passports, photo driving licences and bank statements but not bills. When a patient may not have suitable photographic identification, vouching with confirmation of information held in the medical record can be considered by the data controller or responsible clinician. 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 organisation 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 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 as outlined above
- The identity of the person giving consent for proxy access must also be verified as outlined above. This will normally be the patient but may be someone else acting under a power of attorney or as a Court Appointed Deputy

Child proxy access verification

Before the organisation provides parental proxy access to a child's medical records the following checks must be made:

- The identity of the individual(s) requesting access via the method outlined above
- 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.

How to set up a proxy access

NHS Digital's Linked profiles and proxy access details how to add proxy users to the clinical system to allow parents, family members and carers to access health services on behalf of other people.

Deceased patients

Access to deceased persons medical records

The UK GDPR does not apply to data concerning deceased persons. However, the ethical obligation to respect a patient's confidentiality extends beyond death. There are

several considerations to be considered prior to disclosing the health record of a deceased patient.
Such considerations are detailed in the Access to Health Records Act 1990. Unless the patient requested confidentiality while alive, under the terms of this Act, this organisation will only grant access to either:

- A personal representative (executor of the deceased person's estate); or
- Someone who has a claim resulting from the death

Under section 5(4) of the Access to Health Records Act 1990, no information that is not directly relevant to a claim should be disclosed to either the personal representative or any other person who may have a claim arising out of the patient's death.

It should be noted that the GP contract changed for 2022/23 and has now removed the requirement for practices to print and send copies of the electronic record of deceased patients to Primary Care Support England. Consequently as of 1 August 2022, requests for patients' medical records via the Access to Health Records Act now lie with the organisation.

GP records of deceased patients are retained for 10 years after which time they will be destroyed as detailed within the Records Retention Schedule.

Further detailed information is available within the Access to Deceased Patients Records Policy and the Medical Protection Society article titled Disclosures after death.

Chargeable fees for deceased patients

Legislative changes to the Data Protection Act 2018 have also amended the Access to Health Records Act 1990 which now states access to the records of deceased patients and any copies must be provided free of charge.

However, when health information is to be disclosed for the deceased in the absence of a statutory basis, e.g., when a solicitor or insurance company requests a medical report or information to confirm death or an interpretation of what is in the records, this is classed as private work over and above that which is already available in the record.

Any fees charged should be reasonable and proportionate to cover the cost of satisfying a request.

Further reading can be found in the BMA document titled Access to health records.

Chargeable fees for a SAR

Should a SAR be initiated from a solicitor and they are asking for a report to be written or the request is asking for an interpretation of information within the record, this request goes beyond a SAR and therefore a fee can be charged. The organisation may ask the nature of the request from the solicitor to confirm if this should be charged for or not.

If the solicitor confirms that they are seeking a copy of the medical record, then this should be treated as a SAR and complied with in the usual way.

Fees are further detailed at Section 6.5 and within the BMA webpage titled Access to health records.

Employee requests

Employees and ex-employees of the organisation have a right to request a copy of their personal data including employment record, occupational health records, complaints files, significant event files and any other relevant correspondence. Not all personal data that an organisation holds about an individual needs to be provided as certain exemptions exist. For example, legally privileged documents do not need to be disclosed or when personal data is processed for the purposes of management forecasting or management planning in relation to business planning.

It is also worth bearing in mind that while the ICO advises that employers should be prepared to take reasonable efforts to find and retrieve the requested information, they will not be required to act unreasonably or disproportionately regarding the importance of providing subject access.

The requestor does not need to provide a reason for making a SAR, however they must state who they are and provide appropriate ID. The requestor should specify a date range, subject matter and the people who they believe have sent or received information about them.

An employer cannot refuse to supply information if documents provide third party references. These should simply be redacted on the copy provided to the requestor.

Article 15(1) UK GDPR states that an employer must provide the information requested together with certain additional information.

The additional information includes:

- The purpose for which the employer is processing the data
- Categories of the personal data being processed
- Who receives or has received the personal data from the employer
- How long the employer keeps personal data or the criteria used in deciding how long to keep the information
- Information about where the employer got the personal information from if that information was not collected directly from the employee
- If the employer does cross-border data transfers, information about how data security is safeguarded
- Whether the employer uses automated decision-making and profiling and, if so, details the auto-decision logic used and what this means for the employee

The procedure for employees or ex-employees undertaking a SAR follows the same process as detailed in the section Procedure for Access.

Article 15(3) UK GDPR states that on receipt of a SAR, the employer must give the requestor a copy of their personal information without charge but can charge a reasonable fee for additional requests. If the request is made by e-mail, then the employer must provide

the information in a commonly used electronic format unless the requestor requires the information in a different format.

Further reading can be found in the ICO document titled How should we supply information to the requester?

Denial or limitation of information

Access will be denied or limited when, in the reasonable opinion of the responsible clinician, access to such information would not be in the person's best interests because it is likely to cause serious harm to:

- The person'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 when possible and appropriate, an appointment will be made with the patient to explain the decision.

Third party information

Patient and organisational records 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.

It 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. This will be reviewed and highlighted by the appropriate responsible clinician or data controller. If this is not possible then access to the information will be refused.

Former NHS patients living outside the UK

Patients no longer resident in the UK 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, this organisation may be prepared to provide a summary of the treatment given while resident in the UK.

Disputes concerning content of records

Once access to records has been granted, patients or their proxy may dispute their accuracy or lack understanding of medical codes.

Patients or their proxy may notice and point out errors in their record, unexpected third party references and entries they object to or want deleted. The right of rectification and erasure is established within the UK GDPR.

Any queries will be directed to the data controller who will contact the patient. They will investigate swiftly and thoroughly to identify the source and extent of the problem.

The responsible clinician and Caldicott Guardian/data controller will then decide on the most appropriate action. When the dispute concerns a medical entry, the clinician who made the entry should be consulted and consideration given as to whether it is appropriate to change or delete an entry.

When it is not possible or practical to contact the clinician concerned, the Caldicott Guardian or data controller should be consulted. If it is not possible to amend the records, a meeting with the patient or their proxy should be organised to explain why.

Advice MUST be sought from the DPO should a patient wish to apply their UK GDPR 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)
- Right to object (Article 21 UK GDPR)

When it is not appropriate to amend a medical record, an entry may be made declaring that the patient disagrees with the entry. If the patient further disputes the accuracy once a decision has been made, they will be referred to the complaint's procedure and/or the Health Ombudsman.

Complaints

This organisation has procedures in place to enable complaints about access to health records requests to be addressed and as detailed within the Complaints Procedure.

Specific for data complaints, the complainant may wish to take their complaint direct to the ICO. Alternatively, they may also wish to seek independent legal advice.

Guidance from the DPO should be sought should any data complaint be received.

Care Quality Commission (CQC)

Access to medical records during an inspection

The CQC has powers under the Health and Social Care Act 2008 to access medical records to exercise their role and the Code of practice on accessing confidential and personal information describes its powers that permit accessing medical records.

During any inspection, the CQC inspecting team will look at a patient's medical records

when it is both necessary and intruding on that patient's privacy is justified, proportionate and will protect the privacy and dignity of patients. This is to assess the quality of care provided by the organisation and not to assess the individual clinician.

Further guidance is given within GP Mythbuster 12: Accessing medical records during inspections where it is advised that confidentiality will be maintained of any patient's clinical record and that the inspecting team will always follow its code of practice.

Why the CQC looks at medical records

The CQC inspecting team will assess the quality of care and corroborate its findings through any evidence that it may see within any medical record.

It looks at this evidence alongside:

- Other evidence gathered on the inspection
- Information from the ongoing relationship management with the provider
- Information from the CQC Intelligence Model
- Information gathered before the inspection

As previously detailed, reviews are not designed to assess any individual clinician's ability although should any concerns be identified about an individual clinician then the inspector is duty bound to refer the clinician to their appropriate governing body.

Examples of what may be reviewed

The inspecting team will ensure that several areas are being appropriately considered by the clinical staff within this organisation. All searches have been agreed by the RCGP and the BMA as they represent a reasonable approach to assessing some important features of safe and effective healthcare delivery.

The CQC has provided a detailed list of the records it will review and how it uses the information within its GP Mythbuster.