The Corner Surgery Southport

117 Fylde Road
Southport, PR9 9XP
Tel: 01704 506055
Fax: 0151 247 6238
Email: gp.n84613@nhs.net

Right of Access Policy

Summary

- *Prepared by* Dr David Smith (Data Protection Officer)
- *Effective from* 25th May 2018
- *Last reviewed* 22nd June 2025
- *Next review date* 30th June 2026

Introduction

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/

The right of access allows individuals to be aware of and verify the lawfulness of their data processing.

Under the General Data Protection Regulation (GDPR)/ Data Protection Act (DPA) 2018, individuals will have the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data (and only theirs)
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (*Article 15*).

The GDPR/ DPA 2018 clarifies that the reason for allowing individuals to access their personal data, is so that they are aware of and can verify the lawfulness of the processing (*Recital 63*) and understand how and why the practice is using their data.

"In particular, the public should have straightforward access to clear information about data processing. They should expect the highest standards of transparency for processing that has a serious impact on their lives. We should all be able to see, challenge and correct personal records, especially where these contain detail of particular sensitivity."
ICO, Information Rights Strategic Plan 2017-2021

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

The Data Subject

The Corner Surgery (hereby referred to as 'we', 'us' or 'the practice') has a policy of openness with regard to records. Indeed, health professionals are encouraged to allow patients access to 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 will still apply to such informal requests:

https://webarchive.nationalarchives.gov.uk/ukgwa/20110929153112/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4029974.pdf

There is nothing in the GDPR or DPA that prevents health professionals from informally showing patients (or proxies) their records as long as no other provisions are breached.

A request for access to records in accordance with the GDPR/ DPA 2018 can be made in writing, which includes by email or fax, to the Data Controllers: Drs Mulla and Smith (the practice contract holders). A simple Access Request Form (ARF) will be provided that patients can use if they wish, as appended to this policy.

A request for access to records can also be made as a verbal request, especially if the person that the Data Subject is making the request to can verify his/her identity, e.g. their General Practitioner (GP). Such a request can be made face-to-face or by telephone and in such cases, a written record of such a request should be documented. That written request should then be passed onto either the Practice Manager, Ms Dawn Nicholson or the Information Governance lead, Dr David Smith.

A request does not have to include the phrase 'subject access request' or 'Article 15 of the GDPR' or 'data protection' or 'right of access'.

The requestor should provide enough proof to satisfy the practice of their identity, and the practice is entitled to verify their identity using 'reasonable means'. The practice must only request information that is necessary to confirm who the requestor is.

The default assumption when a requestor asks for 'a copy of their GP record' is that the information requested by the individual is the *entire* GP record. However, the practice may check with the applicant whether all or just some of the information contained in the health record is required before processing the request. The GDPR/ DPA 2018 permits the practice to ask the individual to specify the information the request relates to (*Recital 63*) where the practice is processing a large amount of information about the individual. As a result, the information disclosed can be less than the entire GP record by mutual agreement (the individual must agree so voluntarily and freely). This has sometimes been called a 'targeted' subject access request.

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

It is the practice's policy to request that the Data Subject, who invariably lives locally, collects their information in person. This provides the most secure route of transfer and allows us to verify the identity of the recipient.

In exceptional circumstances (such as if the patient is genuinely housebound, too ill to attend the surgery, or in hospital at the time), the patient can nominate a trusted partner/spouse, relative, friend or neighbour, to collect the records on their behalf.

Secure Online Records Access

The practice can offer, if appropriate, for a requestor to be enabled to securely access their full GP electronic medical record online. This might then allow them to access all of the information that they are be seeking. Recital 63 of the GDPR states:

'Where possible, the controller should be able to provide remote access to a secure system which would provide the Data Subject with direct access to his or her personal data.'

Data Subjects Living Abroad

For Data Subjects living outside of the UK, under GDPR/ DPA 2018 they still have the same rights to apply for access to their records held by the practice. Such a request should be dealt with as for someone making an access request from within the UK.

Next of Kin

Despite the widespread use of the phrase 'next of kin' this is not defined, nor does it have formal legal status. A next of kin cannot give or withhold their consent to the sharing of information on a person's behalf. A next of kin has no rights of access to records.

Representatives of the Data Subject

The GDPR does not prevent an individual from making a subject access request (SAR) via a third party. Often, this will be a solicitor acting on behalf of a client but it could simply be that an individual feels comfortable allowing someone else to act for them.

The practice must be satisfied that the third party making the request *is entitled* to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request.

We are not mandated to disclose that information to anyone else, except where the Data Subject lacks mental capacity when disclosure to a third party would be appropriate – see below. The third party is merely assisting the Data Subject in making the request – the request and the associated subject rights remain with the Data Subject.

Court Representatives

Occasionally, requests for medical records may come from someone who is the 'legal person of the client', such as a Lasting Power of Attorney (LPA) for Health and Welfare or the Court of Protection. In this case, the disclosure *can* be provided to the legal person of the Data Subject as it is likely that disclosure to the Data Subject would be unsafe.

A person appointed by the court to manage the affairs of a person 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 a patient underwent relevant examinations or investigations in the expectation that the information would not be disclosed to the applicant.

However, such disclosures are *not* subject access requests (SARs) - a SAR can only be made by a Data Subject with the requisite capacity. There are no specific provisions in the GDPR or the *Mental Capacity Act 2005* to enable a third party to exercise subject access rights on behalf of such an individual.

On Behalf Of Adults Who Lack Mental Capacity

An individual's mental capacity must be judged in relation to the particular decision being made. If a Data Subject has mental capacity, requests for access by relatives or third parties requires the Data Subject's consent.

When patients lack mental capacity, health professionals are likely to need to share information with any individual authorised to make proxy decisions, such as a LPA for Health and Welfare. Note that an LPA for Property and Finance alone does not provide sufficient authority for an attorney to access a patient's medical records. It should also be noted that even if an LPA for Health and Welfare is in place, an attorney should only be asking for specific pieces of information relevant to the decision being made.

The *Mental Capacity Act 2005* contains powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adult patients. Where there are no nominated individuals, requests for access to information relating to incapacitated adults

should be granted if it is in the best interests of the patient. In all cases, only information relevant to the purposes for which it is requested should be provided.

Again, such disclosures are *not* SARs. A SAR can only be made by a data subject with the requisite capacity to do so.

Children

No matter what their age, it is *the child* who has the right of access to their information, not anybody else. This is the case, even if:

- They are too young to understand the implications of the right of access;
- The right is exercised by those who have parental responsibility for the child; or
- They have authorised another person to exercise the right on their behalf.

Before responding to a SAR for information held about a child, we should consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should usually respond directly to the child. We may, however, allow the parent to exercise the child's rights *on their behalf* if the child authorises this, or if it is evident that this is in the best interests of the child. What matters is that the child is able to understand (in broad terms) what it means to make an access request and how to interpret the information they receive as a result of doing so.

A person with parental responsibility may access the records of a competent child if the child consents. This authority to make a SAR is underpinned by *The Children's Act 1989 Part 1 Section 3*. A person with parental responsibility may seek to exercise any of the child's rights on their behalf. If we are satisfied that the child is not competent, and that the person who has approached us holds parental responsibility for the child, then it is usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf. The exception to this is if, in the specific circumstances of the case, we have evidence that this is not in the best interests of the child.

A person with parental responsibility is either:

- The birth mother; or
- The birth father, if married to the mother at the time of child's birth or subsequently, or listed on the birth certificate from 1st December 2003; or
- An individual given parental responsibility by a court; or
- Adoptive parents, those appointed as a legal guardian, those given a residence order, or those subject to Parental Responsibility Agreements.

Children aged over 16 years are presumed to be competent. A child or your person with capacity has the legal right to access their own health records, and to allow or refuse access by others, including their parents. Children under 16 must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to a SAR (Gillick competency). They must be able to understand, retain, use and weigh up the information they are given, and communicate their decision.

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. One cannot 'veto' access by the other. 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 or objection decisions.

When considering borderline cases, the practice should take into account, among other things:

- The child's level of maturity and their ability to make decisions like this
- The nature of the personal data
- Any court orders relating to parental access or responsibility that may apply
- Any duty of confidence owed to the child or young person
- Any consequences of allowing those with parental responsibility access to the child's or young person's information; this is particularly important if there have been allegations of abuse or ill treatment
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information
- Any views the child or young person has on whether their parents should have access to information about them.

Notification of Requests

The practice will keep a 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.

Fees

In most cases, the practice must provide a copy of the information free of charge, in accordance with Article 12 of the GDPR. The circumstances when a fee can be charged are likely to be rare but include complex requests, i.e. those that are likely to involve a disproportionate amount of GP time to check and redact the record. However, the practice may charge a reasonable fee to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.

Manifestly Unfounded or Excessive Requests

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the practice can:

- Charge a reasonable fee taking into account the administrative costs of providing the information, or
- Refuse to respond.

Where the practice refuses to respond to a request, the practice must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay, and at the latest within one month.

A request may be manifestly unfounded if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purposes other than to cause disruption. Factors that may indicate malicious intent include:

- The individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- The request makes unsubstantiated accusations against you or specific employees;

- The individual is targeting a particular employee against whom they have some personal grudge; or
- The individual systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, e.g. once a week.

These factors are not intended to form a simple tick list that automatically mean a request is manifestly unfounded. We must consider a request in the context in which it is made, and the onus on us is to be able to demonstrate it is manifestly unfounded. In most cases, use of aggressive or abusive language does not, in itself, demonstrate a manifestly unfounded request.

The Information Commissioner's Office (ICO) has stated: *'It is worth noting that 'excessive' is not in relation to the volume of information'*. Whether a SAR is excessive or not depends on particular circumstances. A request may be excessive where it repeats the substance of previous requests and a reasonable interval has not elapsed or it overlaps with other requests. An example of a request that may be excessive is one that merely repeats the substance of previous requests. Requests about the same issue are not *always* excessive though – for example, if the data controller has not handled previous requests properly. The onus is on the Data Controller to prove that the request was 'excessive'.

Requirement to Consult an Appropriate Health Professional

It is the Information Governance (IG) Lead 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 IG Lead must have been consulted and he/she checked the records and authorised the release, or part-release.

It is the responsibility of the IG Lead to ensure that the information to be released:

- Does not disclose anything that identifies any other Data Subject; the only exception to this is the identity of people involved in the care of the individual requestor, such as community staff or hospital specialists
- Does not disclose anything that is likely to result in harm to Data Subject or anyone else
- Does not disclose anything subject to a court order or that is privileged or subject to fertilisation or adoption legislation.

It is important to ensure that records pertaining to another patient have not accidentally been filed in the record. Such records must be removed, both from the information provided within the SAR as well as permanently from the electronic record (and re-filed in the correct patient's GP record, if necessary).

Grounds for Refusing Disclosure to Health Records

The IG Lead should refuse to disclose all or part of the health record if he/she is of the view that:

- Disclosure would be likely to cause serious harm to the physical or mental health of the patient or any other person
- 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
    - Was obtained as a result of any examination or investigation to which the patient consented in the expectation that the information would not be so disclosed, or
    - The patient has expressly indicated it should not be disclosed to that person, or
    - Consisted of 'child abuse data' (personal data consisting of information as to whether the Data Subject is or has been the subject of, or may be at risk of, child abuse) to the extent that the application of that provision would not be in the best interests of the Data Subject
- Disclosure would reveal information that is subject to:
    - A court order, or
    - Human fertilisation and embryology legislation, or
    - Adoption legislation, or
    - Special educational needs legislation, or
    - Parental orders legislation
- The records refer to another individual who can be identified from that information (apart from a health professional). This is unless:
    - The information was provided by the Data Subject (e.g. family history), or
    - That other individual's consent is obtained, or
    - The records can be anonymised, or
    - It is reasonable in all the circumstances to comply with the request without that individual's consent, taking into account any duty of confidentiality owed to the third party.

For the avoidance of doubt, we cannot refuse to provide access to personal data about an individual *simply because we obtained that data from a third party*. The rules about third party data apply only to personal data which includes *both* information about the individual who is the subject of the request *and* information about someone else.

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 medical records because patients may find them upsetting. Where there is any doubt as to whether disclosure would cause serious harm, the IG Lead will consult with a defence body.

Access to Medical Reports Act

The practice will not provide information under a SAR made on behalf of a patient by an insurance agency or employer, and where it is clear that such a request should be made under the Access to Medical Reports Act 1988. This would refer to reports for:

- Employment, proposed or actual, or
- Insurance purposes, i.e. any 'insurance contract', which covers accident claims, insured negligence, or anything covered by an insurance contract that requires a medical report to support an actual or potential insured claim.

If necessary, or unsure, the IG Lead will seek clarification from both the requestor and the patient concerned.

Informing of a 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 practice believes that telling the patient will effectively amount to divulging that information, or is likely to cause serious physical or mental harm to the patient or another individual, then the practice could decide not to inform the patient. In this case 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, and they have the ability to seek to enforce this right through a judicial remedy.

Disclosure of the Record to the Data Subject

Information must be provided without delay and in most cases, *within 1 calendar month*. This is calculated from the day the request is received (which will be day 1).

The period for responding to the request begins at receipt of the request, or:

- When the practice receives any additional information required to confirm the identity of the requestor
- When the practice receives any additional information requested (and required) to clarify the request.

However, The Corner Surgery will follow the following ICO recommendation and strive to provide the information within 28 calendar days: *'For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.'*

Along with the information requested, the additional information that must also be provided (as per Articles 13 and 14 of the GDPR) should be included by means of a copy of the practice's Privacy Notice Leaflet.

If a request is made verbally, for example within a GP consultation, then their GP can – if appropriate and possible within the consultation – provide the requested information immediately.

The practice will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the practice must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Once the appropriate documentation has been received and disclosure approved, the copy of the records may be given to the Data Subject. There should be no circumstances in which it would not be possible to supply permanent copies of health records. When the information requested is handed directly to the Data Subject, then verifiable identification must be confirmed at the time of collection.

Holding a SAR safely at the surgery until the Data Subject can collect it is the most secure way of supplying the information to the Data Subject. In doing so, we have implemented

appropriate organisational and technical measures to ensure that:

- The information remains confidential
- It is accessed only by the individual to whom the data belongs
- There is no accidental loss, destruction, or damage of the record in transit
- The information is processed in a manner that ensures appropriate security and integrity of the personal confidential data requested
- We uphold Article 5(1)(f) of the GDPR.

There are concerns about signed-for packages not being delivered if the Data Subject is not present at home, and the medical record then ending up being stored in a sorting office. Collection from the surgery ensures that the SAR is either in the hands of the Data Controller or the Data Subject, and no-one else in between. The Corner Surgery will move towards providing SARs electronically once we are content with a method that this is both easier for the Data Subject and more secure.

Confidential information should not be sent by email unless:

- The email address of the recipient is absolutely verified, and
- The information is sent *securely;* i.e. encrypted & the password conveyed separately

It should be assumed that if an individual makes a request electronically (i.e. by email), the practice should, if possible, provide that information in a commonly used electronic format (e.g. as .pdf or .doc) and provide it to the requestor.

If sent by post (in exceptional circumstances), the records should be:

- Sent to a named individual by recorded delivery; and
- Marked 'private and confidential, for addressee only'; and
- The practice details should be written on the reverse of the envelope.

<u>The overwhelming majority of patients live locally and there is unlikely to be a valid reason why the contents of a SAR could not possibly be collected in person by the Data Subject (or a suitably authorised person, e.g. family member).</u>

Very rarely, the contents of a SAR might best be provided to the Data Subject by hand-delivering the information. This will only apply where the patient is absolutely and genuinely housebound, and where alternative methods of provision (collection by a trusted third party or securely posted) are not suitable.

The practice is under no obligation to provide records on USB sticks or CD/DVD ROMs

At our discretion, however, we may choose to provide the information in this way but the USB stick or CD/DVD ROM must be new and purchased by the practice, and the data would ideally be encrypted.

Confidential medical records should not be sent by fax unless there is no alternative.

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

A suitable disclaimer would be:

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

Disclosure of the Record to the Third Parties

Many SARs are made by patients with the assistance of third parties, such as solicitors. It should be noted that:

- It is a *Data Subject* access request, not a *third-party* access request
- A third party does not become a Data Subject or 'inherit' Data Subject rights by virtue of making the request on behalf of the individual

It should be noted that the BMA-Law Society consent form [link below] is *not* a request for processing of personal data by means of disclosure to a third party. It is a form to facilitate a Data Subject making a SAR and the request must be treated as such:

https://www.lawsociety.org.uk/topics/gdpr/consent-form-access-to-client-health-records

There are very limited circumstances where disclosure to a third party is almost certainly required; for example, if the Data Subject is in prison or in hospital abroad, or if a patient lacks capacity and the request is made by someone with an active, in-force LPA for Health and Welfare. In addition, where the Data Subject is a child the information should be provided to the person so authorised to have made the request on their behalf.

In all other circumstances, once the SAR has been prepared and is ready for disclosure, the practice will assess whether disclosure directly to a third party, if so requested, is justifiable, appropriate, lawful and reasonable, for that particular SAR. All such assessments are made on an individual SAR basis. It would be wrong to have a blanket policy of *never* supplying third parties with a data subject's SAR.

However, the practice may well have *one or more concerns* regarding the disclosure to the third party, such as that:

- We *could* be disclosing excessive information – that is, the records requested *may* go far beyond that necessary for the intended purpose;
- The Data Subject would not in a position to be aware of, and to verify, the lawfulness and nature of the processing of their personal data, in line with Article 63 of the GDPR;
- The Data Subject would not be in a position to exercise their right to object to aspects of processing of their personal data;
- The Data Subject would not in a position to determine the accuracy of their GP medical record and, if so needed, exercise their right to rectification
- The Data Subject would not be in a position to consider whether the processing of personal data relating to him or her infringes the GDPR and so exercise their right to lodge a complaint with a supervisory authority;
- The Data Subject would not be in a position to determine whether there was personal confidential information that they did not wish to share with a third party;
- Sections 184 and 185 of the DPA 2018 afford the Data Subject important protections and safeguards (against 'enforced access) for their confidential medical information

which would be bypassed, to their detriment, were we to disclose their SAR directly to a third party;
- If the Data Subject is a claimant in a legal matter, they would be unaware of the information that might be, or would have to be, disclosed by their solicitor (i.e. 'served') to the defendant's legal representative;
- Failing to provide a copy of the data to the Data Subject would mean that were the data subject, or any third party on their behalf, to request another copy of the SAR from us following this request, we would be entitled to charge for doing so;
- The data subject will not be in control of their own medical information.

It should be noted that disclosing a SAR directly to a third party would neither be:

- Providing the data subject with a copy of *their* personal data, nor
- Allowing the data subject access to *their* personal data, nor
- Enabling the data subject to find out:
    - What personal data we hold about them
    - How we use their personal data
    - Who we share their personal data with
    - Who has access to their personal data
    - Where we obtained their personal data from

…which would be a contravention, by us, of Article 15 and the principles of Recital 63 of the GDPR. Disclosing a SAR directly to a third party would *not* be upholding the principles of the ICO's 'Your Data Matters' campaign: *'Your right to access means you can ask to see the data an organisation holds on you, and to verify the lawfulness of its processing.'*

Accordingly, should the practice have *any* such concerns, the SAR should be provided directly to the Data Subject, as it is *their* Data Subject right of access. This will allow them to make their own choice about what information they pass on to any third party.
GP surgeries do not take 'orders' or 'instructions' from patients.

We *are* mandated to provide the Data Subject with their SAR and uphold their right of access. That is a *legal obligation*. We *are not* mandated to transfer/disclose personal confidential medication information to a third party as a result of a Data Subject's access request. That would be *processing of data* from one controller to another controller. There are no provisions in Article 15 of GDPR, and no requirements under data protection law, whereby:

- We are compelled to process personal confidential information in that way – unless 'legal obligation' is the legal basis for such processing, we cannot be forced to disclose the SAR to a third party, or
- A SAR is lawfully fulfilled by bypassing the Data Subject and disclosing (i.e. *processing*) their personal data to a third party, or
- Data Subject rights are 'transferred to' or 'inherited by' a third party assisting a Data Subject in making their request, or
- A Data Controller-Subject relationship is generated between the GP surgery and the third party assisting an individual making a SAR.

An organisation, such as a firm of solicitors, cannot make a Data Subject access request or be a Data Subject, because a Data Subject is a *'natural' person or individual* who is the subject of personal data; that is, an 'identified or identifiable living individual to whom personal data relates':

http://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted

A form of authority from a patient does not, nor cannot, "set aside" the Data Subject's right of access, nor does it "set aside" the Data Controller's legal obligation to the Subject under Article 15.

It is clear that our obligation as Data Controllers is to 'supply' or 'provide' the Data Subject (the requester) with the SAR, not to 'send' it to them:

'The focus of a subject access request (SAR) is usually the supply of a copy of the requester's personal data' - Subject Access Code of Practice, ICO 2017

'The Data Controller must provide the Data Subject with a copy of the personal data being processed' - Handbook on European Data Protection Law, EU FRA/CoE/EDPS 2018

According to the Hessian Supervisory Authority (SA), the Data Controller must always provide the Data Subject a copy of the personal data, even if the Data Subject does not explicitly request a copy. We should also be mindful of the National Data Guardian's guidance on the use of healthcare data, in particular that: *'There must be no surprises to the citizen about how their health and care data is being used'*. This would apply to *which* organisations receive or have access to a patient's personal confidential information, and also *exactly what* from their GP record is being disclosed or given access to.

Ensuring that the data subject receives their SAR fully upholds the GMC's eighth principle of their confidentiality guidance:

'Support patients to access their information. *Respect, and help patients exercise, their legal rights to be informed about how their information will be used and to have access to, or copies of, their health records.'*

Data Retention Policy

All SAR information – whether printed out or stored electronically – will be kept for a maximum of 12 months or until the following 1st January, whichever is later, before being permanently destroyed/deleted.

Legal Bases

The upholding of the right of access is a legal obligation.

Disclosure of the personal confidential medical information is processing, and as such require legal bases:

- Article 6(1)(c) : legal obligation
- Article 9(2)(h) : official authority

If disclosure is made *directly to the data subject,* then the common law of confidentiality is not involved.

Dr David Smith

The Corner Surgery
Southport

117 Fylde Road
Southport, PR9 9XP
Tel: 01704 506055
Fax: 0151 247 6238
Email: gp.n84613@nhs.net

Recording Access Requests Made Verbally - In Person or By 'Phone

Date of request:	
How was it made?	□ Face to Face □ By Telephone

Details of the Data Subject (patient or employee)

Full name:			
Address & postcode:			
Telephone number:		Date of birth:	

Details of the person who wishes to access the data, if different from the above

Full name:	
Address & postcode:	
Telephone number:	
Relationship to Subject:	

□ I have positively identified the requestor OR □ I have requested formal identification

What does the request relate to & what exact information do they require?

[e.g. key events, past history, relevant dates]

Is this a request for a patient's *entire* GP medical record?	□ Yes □ No	How would they *prefer* to receive the information?	□ Collection □ Post □ Email

Remind the requestor that he/she might be contacted by the practice for further information or clarification of the request, if needed. Then pass this request on to the Practice Manager, Ms Dawn Nicholson or Information Governance Lead, Dr David Smith

The Corner Surgery
Southport

117 Fylde Road
Southport, PR9 9XP
Tel: 01704 506055
Fax: 0151 247 6238
Email: gp.n84613@nhs.net

Access Request Form

By completing this form, you are making a request for information that the practice holds about the Data Subject, under the relevant legislation:

General Data Protection Regulation; and/or Data Protection Act 2018; and/or Access to Health Records Act 1990; and/or Access to Medical Reports Act 1988

Details of the Data Subject (patient or employee)

Full name:			
Address & postcode:			
Telephone number:		Date of birth:	

Details of the person who wishes to access the data, if different from the above

Full name:	
Address & postcode:	
Telephone number:	
Relationship to Subject:	

Please specify what the request relates to & the exact information you require:

[e.g. relevant dates, specific events, medical conditions, hospital letters, or all records]

I am [*please select that which applies*]:

☐ the Data Subject

☐ the Data Subject's representative

Signed: .....

Name: .....

Date: .....

In most cases, we will be able to complete your request within 28 days; we will let you know if this is not going to be possible. In some cases, we will require further information to process the request and there may be a charge; we will let you know as soon as possible.

For reception use only:

- I have checked the signatory's photo ID ☐ and proof of address ☐ ..... [*initials*]