Subject Access Request/Right of Access Policy for patients

Contents

The "Right of Access"

The right of access[1] allows individuals ("Data Subjects") to access information about the Personal Data an organisation (the "Data Controller") holds about them.

The purpose of this right is to allow individuals to access their personal data so that they are aware of, and can verify, the lawfulness of the processing and understand how and why the Practice is using their data[2].

For the purposes of this document the Practice is the Data Controller, and the individual is the Data Subject.

The right of access applies to all data the Practice holds about a patient, including data within your clinical systems, emails, telephone recordings, CCTV and any paper records you hold.

Individuals have the right to the following information:

- confirmation that their data is being processed by the Practice.
- access to (and a copy of) their personal data.
- other supplementary information (which should already be available from your privacy notice) comprising:

    - the purposes of the processing
    - the categories of personal data concerned
    - the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
    - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
    - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
    - the right to lodge a complaint with a supervisory authority
    - where the personal data are not collected from the data subject, any available information as to their source
    - the existence of automated decision-making, including profiling

Personal Data

Personal data is defined under GDPR Article 4 (1) as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an

[1] Article 15 of GDPR "Right of Access by the Data Subject" https://gdpr-info.eu/art-15-gdpr/
[2] Recital 63 of GDPR "Right of Access" https://gdpr-info.eu/recitals/no-63/

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

As such, it must relate to a living individual and contain context or information that would allow that individual to be identified from it.

Requests for Access

Request for access can be made by the patient, or their nominated representative(s) (see requests from patients representatives and third parties).

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

The Practice may ask the individual to specify the information the request relates to and whether all or just some of the information contained in the health record is required before processing the request.

Similarly, the patient can request data from a specific time period, or in relation to a specific condition or treatment they received.

A request for access to health records in accordance with the GDPR/DPA 2018 can be made in writing, which includes by email or fax, but can also be made as a verbal request, face-to-face or by telephone. In the case of a verbal request, a written record of this should be documented.

A simple form is available as part of the SAR procedure that patients can use if they wish, however they cannot be compelled to use this.

A request does not have to include the words "subject access request", "SAR", "GDPR" etc. to be considered a valid request.

Fees for Subject access requests

An initial copy of the information must be provided **free of charge**.

A reasonable fee may charged to comply with requests for further copies of the same information- this fee is based on the administrative cost (paper, consumables, admin time, clinician time for reviewing notes etc.) of providing this information.

Time limit for responding

The SAR must be fulfilled within one month (although the NHS target date is 21 days) from the day the request is received (if clarification of the request is required or confirmation of identity needed, then this will be classed as the date the request was received).

If it is not possible to provide the records within the specified one month for a valid reason such as complexity or availability of records, then the period allowed can be

extended for a further two months, however the patient **must** be informed of this within the original one month timescale.

Confirming and verifying the requestor's identity

The patient should provide enough proof to satisfy the Practice of their identity and the Practice must only request the minimum amount of information that is necessary to confirm who they are.[3]

Requests directly from the Patient

There is nothing in the DPA18 or GDPR that would prevent a health professional from informally showing the patient (or their nominated representative) their record as long as no other provisions of data protection legislation are breached, however these instances should be recorded in the health record. Please note that allowing the patient to view their notes will not discharge all the responsibilities of the Right of Access

Requests from Patient Representatives and third parties

The GDPR does not prevent an individual making a subject access request via a third party.

In these cases, the Practice needs to 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.

It is the policy of the Practice to only disclose the contents of a SAR directly to the data subject.

Under GDPR, the Practice is not mandated to disclose the content of the Subject Access Request to anyone else but the data subject (except where the data subject lacks capacity, when disclosure to a third-party may be appropriate – see requests on behalf of adults who lack capacity).

In all cases, the third party is acting on behalf of the data subject.The request, the data and the rights over that data will always remain with the Patient, not the representative.

The Practice cannot he held responsible for how the data is disseminated after it has been released to the patient.

[3] GDPR Recital 64 "Identity Verification" https://gdpr-info.eu/recitals/no-64/

Next of Kin

"Next of kin" does not have formal legal status in data protection legislation and "next of kin" cannot give or withhold their consent to the sharing of information on a patient's behalf and have no automatic rights of access to medical records

Requests on behalf of adults who lack capacity

The Mental Capacity Act 2005 contains provisions for individuals to be nominated to make decisions regarding health and welfare on behalf of adults who lack capacity and information can be shared with any individual authorised to make proxy decisions (such as lasting power of attorney), however only information relevant to the specific health or welfare purposes for which it has been requested should be released.

If a patient has adequate capacity, requests for access by relatives or third parties will require their consent.

Where no individuals are nominated to make decisions on behalf of the patient, requests for access should be granted only if it is in the best interests of the patient and only relevant information should be provided.

Requests for access to the records of minors

Regardless of age, the right of access belongs to the individual and before release of records, the capacity of the minor to understand their rights, must be considered.

If the minor is mature enough (i.e. Gillick competent) to understand the purpose and meaning of the request, then the records should be released to the minor.

The person with Parental Responsibility may access the records of a competent minor if the minor consents to this..

If the minor is not sufficiently mature, or are aged under 16, then individuals with Parental responsibility can exercise this right on behalf of the minor if it is thought that this is in their "best interests"

Children aged over 16yrs are assumed to be competent, unless there is a specific reason why this is not the case.

It is considered good Practice that a Gillick competent minor should be actively encouraged to discuss any subject access related decisions with those with Parental Responsibility.

In these situations, consideration should be given regarding:

- The minor's level of maturity and their ability to understand this type of request
- The contents of the record
- The duty of confidence owed to the child or young person
- Any court orders that may be in place relating regarding Parental responsibility

- 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; and
- Any views the child or young person has on whether their parents should have access to information about them.

Parental responsibility in England is not an automatic right for all parents, but is automatically given to

- The birth mother
- The birth father, if they are married to the mother at the time of minor's birth, or before the registration of the birth
- Fathers who are not married to the birth mother will have automatic Parental responsibility if:
  - their child was born on or after 1 December 2003 (which should now be the case for all minors), and
  - their name is on the birth certificate

Parental responsibility may be given or removed by the courts (using legal mechanisms including "Parental Responsibility Agreements") so can also be held by:

- Adoptive parents
- Legal guardians
- Biological fathers who did not automatically receive Parental responsibility at their child's registration,
- Spouses/civil partners of individuals with Parental Responsibility ("step parents")
- Those to whom a Family Courts Residence Order has been awarded

Parental Responsibility will not be affected by the divorce or separation of those with Parental Responsibility, unless the courts deem otherwise.

When more than one person has Parental Responsibility, each may independently exercise the Rights of Access on behalf of the minor regardless of their current domestic status.

If a request is made by an individual with Parental Responsibility, it may be sensible to inform any other individuals with Parental Responsibility of the request in order to prevent duplication of information (and possible costs to the individual for supplying the same information), however in situations where there are reasons for concern such as safeguarding or domestic violence, then there is no obligation to inform any other individuals with Parental Responsibility.

Parental Responsibility is not routinely given to foster parents (in these cases Parental responsibility will generally be assigned a local authority), although they are classed as "Direct Care Givers" so a partial right of access, for instance to recent test results

relevant to a clinical condition, might be considered as being in the patient's "best interest".

Requests from members of Parliament

Under section 190

Requests from Representatives appointed by the courts

Subject access requests may come from an individual who has been appointed by the courts as a representative of the patient, by a power of attorney or Court of Protection, to manage the affairs of a patient who is incapable of managing his or her own affairs.

In this case, the SAR can be provided directly to the "legal person" of the data subject, however, access may be denied, or redactions made, where the GP is of the opinion that the patient underwent any treatment in the expectation that this treatment would not be disclosed to anyone else, including their representative.

Requests from Patients who have left the Practice

Former patients who have left the Practice may still have the Right of Access due to the legacy nature of some clinical systems and these should be treated in the same way as requests from registered patients, although in some cases it may not be possible for these records to be accessed. Patients should however be advised that they could get a more up to date version of these records from their current GP.

Requests from Patients living abroad

For former patients living outside of the UK (whether still in the EU or elsewhere), under GDPR/DPA 2018 they still have the same rights to apply for access to their UK health records. Such a request should be dealt with as someone making an access request from within the UK.

Requests for the records of deceased patients

Request for access to the record of deceased patients do not fall under the Right of Access in GDPR/DPA18 (this legislation is only applicable to living individuals).

Access to these records is governed by the Access to Health records Act 1990[4] which allows for limited access to the record of deceased patients, with the some of the similar caveats as for the records of living individual and access can be refused if it would be likely to cause serious harm, or would identify third parties.

NHS England is the current "Data Controller" (insofar as this term can be applied outside GDPR/DPA18) for these records and although you may still have computerised records for these patients the official guidance is for individuals to apply via PCSE for access to these records. Access to these records is limited to:

[4] https://www.legislation.gov.uk/ukpga/1990/23/contents

- A deceased patient's personal representative – i.e. the executor/administrator of their will or estate
- Someone with a claim arising from the death of the patient, such as someone contesting the validity of a will on grounds of testamentary capacity or someone making a claim against the estate.

Requests from the Legal Profession

Requests are often received by solicitors on behalf of patients.- In this situation they act as the "Patient Representative" outlined above, however, it is important to remember that the purpose of the Right of Access is to allow data subjects (patients) to obtain information regarding the data held about them, access that data, verify its accuracy and exercise their rights under GDPR/DPA18.

The Right of Access was not developed to bypass the data subject and facilitate disclosure, at no cost, of personal information directly to a solicitor for legal purposes- there are other legal avenues for this that do not misuse the data rights of individuals.

ICO guidance regarding Subject Access requests made on behalf of patients by third parties[5] states:

"If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it."

By definition the individual cannot know or understand until they have seen it in its entirety what information will be disclosed, so the information will be provided to our patient in the first instance, and they can make appropriate decisions on further sharing of that information with third parties.

Requests from Insurance Companies

The Practice will not provide information under a Subject Access Request made on behalf of a patient by an insurance agency, and such a request should be made under the Access to Medical Records Act 1988[6]- this would refer to reports for insurance purposes (accident claims, negligence. life insurance, mortgages etc.)

As above, the Right of Access was not developed to bypass the data subject and facilitate disclosure, at no cost, of personal information directly to an insurer to underpin their commercial Practices- there are other legal avenues for this that do not misuse the data rights of individuals.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
[6] https://www.legislation.gov.uk/ukpga/1988/28

Requests from Employers

The Practice will not provide information under a Subject Access Request made on behalf of a patient by an employer (proposed or actual) for employment purposes, and where it is clear that such a request should be made under the Access to Medical Records Act 1988.

As above, the Right of Access was not developed to bypass the data subject and facilitate disclosure, at no cost, of personal information directly to an employer to underpin their commercial Practices- there are other legal avenues for this that do not misuse the data rights of individuals..

Requirement to consult an appropriate health professional

Before any Subject Access request is released to the patient, or their nominated representative, the content must be reviewed by one of the Practice's GPs to ensure that the information to be released:

- Does not disclose anything that identifies any other data subject. The only exceptions to this are:
    - The identity of health Care Professionals (Drs, nurses, community staff, but not admin staff) involved in the medical care of the patient.
    - The identity of any third parties provided to you by the data subject (please see sections below for further information).
- Does not disclose anything that is likely to result in harm to the data subject or anyone else
- Does not disclose anything subject to a court order or that is otherwise privileged
- Does not disclose anything subject to fertilisation or adoption legislation

Grounds for refusing access to health records and redacting records

The Practice can refuse to disclose all or part of the health record if it has been decided that:

- Disclosure would be likely to cause serious harm to the physical or mental health of the patient (or any other person)[7]
- The records refer to another individual who can be identified from that information (apart from a health professional)[8] unless:

[7] http://www.legislation.gov.uk/ukpga/2018/12/schedule/3/paragraph/5/enacted
[8] http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/3/enacted

- the identity of the individual was provided by the data subject, or
- that other individual gives consent, or
- the records can be anonymised and the details fully redacted, or
- it is reasonable to comply with the request without the third party's consent, taking into account:
  - any duty of confidentiality that may be owed to the third party
  - the type of information that would be disclosed

- 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[9], and:

  - the information was given by the patient in the expectation that it would not be disclosed to the person making the request; or
  - the patient has expressly indicated it should not be disclosed to that person

Circumstances in which information may be withheld on the grounds of serious harm should be rare, and this exemption does not justify withholding coded entries, free text, comments etc. held within the record because patients may find them upsetting.

Where there is any doubt as to whether disclosure would cause serious harm, it is recommended that the GP discusses the matter with their Caldicott Guardian or defence body.

Third Party Data and redaction

The presence of third party information in the record does not remove or negate the right of access.

Third party data will not be disclosed via SAR i.e. if the record refers to another individual who can be identified from that information (apart from a health professional, or other "relevant" professional), unless the conditions listed below from Schedule 2 Part 3 apply[10]:

(2)Sub-paragraph (1) does not remove the controller's obligation where—
(a)the other individual has consented to the disclosure of the information to the data subject, or
(b)it is reasonable to disclose the information to the data subject without the consent of the other individual.

(3)In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including—
(a)the type of information that would be disclosed,
(b)any duty of confidentiality owed to the other individual,

[9] http://www.legislation.gov.uk/ukpga/2018/12/schedule/3/paragraph/4/enacted

[10] http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/16/enacted

(c)any steps taken by the controller with a view to seeking the consent of the other individual,
(d)whether the other individual is capable of giving consent, and
(e)any express refusal of consent by the other individual.

The ICO recommends a three step process for ascertaining whether data can be released

Step 1- does the request require the disclosure of Information that identifies a Third Party?

The Practice should consider if it is possible to comply with the request without revealing information that relates to and identifies and Third Party- in doing so, it should be taken into account the information you would have to disclose and any information that you could expect the recipient of the request to be able to obtain that might identify the individual

If it is not possible to separate the third party information from the request and still comply then Step 2 needs to be considered.

Step 2- Has the Third Party consented?

If possible, you can ask the Third Party for their consent for this data to be released. It is recognised that in Practice this is very likely to not to possible or feasible and there is no absolute obligation to obtain consent. Consent would not be required if the information is already known to the requestor.

Step 3- Would it be reasonable to comply with the request without consent?

If you are unable to get consent (either the Third party has refused, or cannot be located) or it has not been feasible to get consent (because in doing so you would have to reveal personal data about the requestor to the Third party) then you can consider if it is appropriate to disclose without consent. A list of factors to be taken into account under these circumstances is listed in Sch2 part 3 above.

It is therefore sometimes possible to disclose information relating to a third party, however, it will need to be decided on a case by case basis whether this is appropriate.

In summary, Third Party data could be released where the data

- Has previously been provided by the data subject to you
- Is already known to the data subject
- Is already “public knowledge”
- The third party consents to this
- It is reasonable in all the circumstances to disclose without consent

The caveats regarding Third Party data will only apply personal data which includes both information about the individual who is the subject of the request, and information about

someone else- for practical examples of how this might apply please see appendix 1 to this document.

When disclosing coded family history recorded within the GP record, unless you are certain that this information was provided directly from the data subject, it should be redacted as it is possible that this was entered directly into the record because of “prior knowledge”.

One other area that requires specific attention is the possible release of any contact details (address, phone number etc.) of one individual with Parental Responsibility, in a SAR released to another individual with Parental Responsibility – particularly where the other parent is “estranged” or there are safeguarding concerns.

Be aware that hospital letters and discharge notes will often contain contact details, of both the patient and in many cases the “next of kin”. In many cases the next of kin details will have been provided to the hospital directly by the data subject, but redact these if necessary.

For secure online records access, any documents or entries containing information that needs to be redacted or withheld will need to be made “not visible online”.

Informing of the decision not to grant access

The decision not to grant access can only be taken by the GP and this should be noted, with the reasons and appropriate justification as to why.

If you decide not to grant access you should inform the patient or their representative, if they do not have capacity, within 28 days.

However, if you think that telling the patient that they cannot be granted access due to the risk of serious harm to the patient or any other person, and the reasons why you cannot grant this:

- Would effectively amount to divulging that information; or
- May itself cause serious harm to the patient or another individual

Then you could choose not to inform the patient of your reasons for not allowing access, in which case this should be noted.

Although there is no right of appeal to this, it is the Practice’s policy to give a patient the opportunity to have their case investigated via the complaints procedure.

The patient must be informed in writing that every assistance will be offered to them if they wish to do this.

If the Practice complaint procedure is exhausted and the patient remains unsatisfied, the patient may also complain to the ICO for an independent ruling on whether access should be granted.

Disclosure of the record

Release directly to patient

It is the policy of the Practice to provide the SAR directly to the data subject.

Once the appropriate documentation has been received and the SAR approved, this can be given to the patient, providing valid ID documentation is produced

In addition to the information within the SAR, the other information listed under Article 15 of the GDPR must also be supplied. This is included within the SAR request from, or by directing the patient to the Practice Privacy Notice.

Release of paper copies of the record

It is the Practice policy to request that the data subject collects their information from the surgery in person, as this provides the most secure route of transfer and allows the Practice to verify the identity of the recipient.

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

Release by Email

SARs can be released to the patient via email, provided that the email address has been adequately verified. The email must be sent from a Practice NHS.Net address and using the “SECURE” function.

The Practice cannot accept responsibility for the security of the patient’s email address.

Release supplied on other media

The Practice is under no obligation to provide SAR on removable media such USB drives or disks.

The Practice may agree to supply information in this manner (for instance if the record is particularly lengthy) but the removable media will be supplied by the Practice- the Practice will not accept blank media devices for patients due to potential security risks.

Whenever possible the removable media must be fully encrypted.

Secure Online Records Access

The Practice can arrange for online access to be enabled to allow the patient to securely access their record online.

This will discharge the obligations of Article 15 only if the patient is offered access to the full record (including historic data and free text) and the entirety of the record is summarised and the additional information required to meet the obligations of Article 15 can is supplied.

Release by post

Release of the SAR by post should only be in exceptional circumstances (only when the patient in genuinely housebound and other options are not available) and the following must be in place:

- the record should be sent to the named patient
- should be posted by recorded delivery, where the item(s) are signed for..
- marked “private and confidential- for addressee only”
- Practice details should be supplied.

As patients should live locally to the Practice patient (or their representatives) are encouraged to collect records personally, so that ID can be verified.

Recording of Subject Access Requests

The Practice will keep a central record of all requests in order to ensure that requests are cross-referenced with any complaints or incidents and that the deadlines for response are monitored and adhered to.

Manifestly unfounded or excessive requests

There is provision within GDPR/DPA18 for Practices, when requests are manifestly unfounded or excessive, to:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond

Currently there is little guidance as to what “manifestly unfounded or excessive” would mean (with the exception of a request for information which has already been released) and if a Subject Access Requests was believed to fall within the this definition for reasons of size or complexity, then the ICO should be consulted for advice

Data retention policy

All SAR information – whether printed out or stored electronically – will be kept for a maximum of 12 months before being permanently destroyed/deleted.

Appendix 1

Practical examples of third party data and redaction

The caveats regarding Third Party data will only apply personal data which includes both information about the individual who is the subject of the request, and information about someone else.

This decision will involve balancing the data subject's right of access against the Third Party individual's rights- for example an entry in the patient's medical record stating "*Mother attended surgery to voice concerns about the patient"* - There is no personal data about the mother and you cannot refuse to disclose that information under SAR, unless this would cause harm to the patient.

An entry stating "*Brother emailed me to say that he is worried about the patient's back pain as he (the brother) was diagnosed with prostate cancer 6 months ago"* does contain personal information about the Third Party and should be redacted from the record unless the third party has given their permission.

Another other matter to consider is the source of the information about a third party. If you are disclosing the SAR directly to the data subject, when checking if the record contains third party information it is important to ascertain (as far as possible) where that information originated.

For example if a letter from a clinic stated that the patient had told a consultant "*patient tells me that his brother was diagnosed with cancer aged 50*" the information in this case was supplied by the data subject. It would not in this case be necessary to redact that information, as it was already known to the patient and was supplied by the patient.

It would however be required that this information was redacted if you were disclosing this to a third party who requested the SAR on behalf of the patient, were disclosing to the police as a voluntary disclosure or other similar disclosure involving a third party.

A letter from a clinic containing text such as "*I recall treating his brother for cancer"*" should be treated differently as in this case, the third-party information was not provided from the patient – and so should be redacted regardless of who the record is being released to.

If, in a referral letter about the data subject, you make reference to "*her sister, also my patient, was diagnosed with ovarian cancer last year*" then clearly that information should be redacted – that information did not come from the data subject, and contains confidential medical information, and you clearly have a duty of confidentiality to the sister (who is also your patient).