OAKLEY HEALTH GROUP	
RIGHT OF ACCESS POLICY (*Subject Access Request, "SAR", "DSAR"*)	
REVIEW DATE:	**12.05.21**
REVIEWED BY:	**Dr N Bhatia**
NEXT REVIEW:	**01.10.21**

Introduction

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

The right of access allows individuals to be aware of and verify the lawfulness of the processing,

Under the GDPR, 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 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 health records may be made in any of the circumstances explained below.

The Patient

Oakley Health Group (hereby referred to as "we" or "the Practice") has a policy of openness with regard to health records and health professionals are encouraged to allow patients to access their health records on an informal basis. This should be recorded in the health record itself. The Department of Health's Code of Practice on Openness in the NHS will still apply to informal requests.

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

A request for access to health records in accordance with the GDPR can be made in writing, which includes by letter, email, or e-consult, to the data controller, i.e., the Practice. A simple form will be provided on our website that patients can use *if they wish* (and as appended to this policy).

A request for access to health records in accordance with the GDPR can also be made as a verbal request, especially if the person (that the patient is making the request to) can verify his/her identity (e.g., their 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 or the Information Governance lead.

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 requester 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 they are.

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 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 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.

It is Oakley Health Group's policy to request that the data subject (who invariably lives locally) normally collects their information from one of the three surgeries in person, as 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, or 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 record online. This would then allow them to access all information that they might be seeking. This is permissible because the Practice offers *full* access to the GP electronic record (including historic data and free text).

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."

Patients living abroad

For former patients living outside of the UK and whom once had treatment for their stay here, under GDPR 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.

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 patient's behalf. A next of kin has no rights of access to medical records.

Patient Representatives

The GDPR does not prevent an individual making a subject access request *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. 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.

We are not mandated to disclose that information to anyone else but the data subject. The third party is merely "assisting" the data subject in making the request – the request, and the associated subject rights, remain with the patient.

Court Representatives

Occasionally, requests for medical records may come from someone who is the "legal person of the client", such as achieved by a registered power of attorney (LPA for Health and Welfare) or the Court of Protection (court appointed deputy for health & welfare).

In this case, disclosure *can* be provided to the legal person of the data subject, and indeed should 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 patient who is incapable of managing his or her own affairs may make such a request. Access may be denied where the GP is of the opinion that the patient underwent relevant examinations or investigations in the expectation that the information would not be disclosed to the applicant.

But such disclosures are not SARs – a SAR can only be made by a data subject (with the requisite capacity).

There are no specific provisions in the UK GDPR, or the Mental Capacity Act 2005, enabling a third party to exercise subject access rights on behalf of such an individual.

Individuals on behalf of adults who lack capacity

An individual's mental capacity must be judged in relation to the particular decision being made. If a patient has capacity, requests for access to medical records by relatives or third parties require his or her 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 an individual acting under the authority of a lasting power of attorney for health & welfare.

Note that LPA for Property and Finance *alone* does not provide sufficient authority for an attorney to access a patient's medical records (see Appendix 1).

It should also be noted that even if a Health & Welfare LPA was in place, an attorney should only be asking for specific pieces of information relevant to the decision being made. A GP would be within their rights to deny blanket access.

The Mental Capacity Act in England and Wales contain powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults.

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.

And, 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 their age, it is *the child* who has the right of access to their information.

The right to access information we hold about a child is the child's right rather than anyone's else's, 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 subject access request 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 a subject access request and how to interpret the information they receive as a result of doing so.

A person with parental responsibility (see below) may access the records of a competent child if the child consents.#

Such authority (to make a SAR) is underpinned by The Children's Act 1989 Part 1 Section 3:

http://www.legislation.gov.uk/ukpga/1989/41/section/3

An adult 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.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/#a4

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

Parental responsibility is not necessarily automatic for all parents.

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)

However, in both cases, this can be removed by the court.

Unmarried fathers will only have automatic parental responsibility if:

- their child was born after 15 April 2002 (Northern Ireland), 1 December 2003 (England and Wales) or 4 May 2006 (Scotland)

  AND

- the father's name is on the birth certificate

Parental responsibility can also be held by adoptive parents, those appointed as a legal guardian or those given a residence order.

Additionally, when a child is subject to a care order, parental responsibility will be held by the local authority.

Parental responsibility may be acquired or awarded, and it may also be removed by a court order.

Stepparents do not automatically have parental responsibility (e.g. a man marrying the birth mother).
A civil partner will have parental responsibility if they are named on the child's birth certificate.

Unmarried fathers, or civil partners, who are not named on the birth certificate, or stepparents, can acquire parental responsibility if they obtain

- a Parental Responsibility Agreement from the child's mother, or
- a Parental Responsibility Order from the court

This all may require us to ask to see proof of identity, and/or evidence of parental responsibility, or proof that the court has withdrawn parental responsibility.

Divorce or marital separation does not affect parental responsibility. However, it can be restricted by the court.

When more than one person has parental responsibility, each may independently exercise rights of access.

Adoptive parents usually have parental responsibility.
If a child is adopted, the birth parents lose parental responsibility.

Representatives of the local authority have parental responsibility for a child who is in their care.
They may share this responsibility with the parents of the child.

A child's testamentary guardian, special guardian or other person given a residence order also has parental responsibility.

(This is not an exhaustive list but contains the most common circumstances).

If the appropriate health professional considers that a child patient is Gillick competent (i.e., has sufficient maturity and understanding to make decisions about disclosure of their records) then the child should be asked for his or her consent before disclosure is given to someone with parental responsibility.

Children aged over 16yrs are presumed to be competent. A child or young 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 (in England) must demonstrate that they have sufficient understanding (capacity) of what is proposed in order to be entitled to make or consent to an SAR (Gillick competency). They must be able to:

- understand, retain, use and weigh the information they are given
- communicate their decision

Capacity does not entirely depend on the child's age. It rests more on their ability to understand and weigh up options.

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.

It may be wise to make sure the other parent is aware of the request, so that we can take into account any objection they may make and the reasons for it.

In all circumstances good practice dictates that a Gillick competent child should be encouraged to involve parents or other legal guardians in any treatment/disclosure decisions.

If the child does not have capacity, we always need to consider if it is in the child's best interest to disclose the information.

Notification of 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.

Fees

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 for access to health records are likely to be rare but include "complex" requests (likely to involve a disproportionate amount of GP time to check and redact the record).

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, should we choose to respond; 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
- 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 means 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 ICO has stated: *"it is worth noting that 'excessive' is not in relation to the volume of information."*

In most cases, a request is not excessive just because the individual has asked for a large amount of information, even if we find it a burden.

Whether a request is excessive or not depends on its particular circumstances. A request may be excessive if it:

- repeats the substance of previous requests and a reasonable interval has not elapsed; or
- 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. An individual may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the 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 GP's responsibility to consider an access request and to disclose the records if the correct procedure has been followed. Before the Practice discloses or provides copies of medical records the patient's GP (or the Information Governance lead) must have been consulted and he / she checked the records and authorised the release, or part-release.

It is the responsibility of the GP 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 the 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 GP should refuse to disclose (i.e., *exempt)* all or part of the health record if he/she is of the view that either:

- Disclosure would be likely to cause serious harm to the physical or mental health of the patient or any other person
  http://www.legislation.gov.uk/ukpga/2018/12/schedule/3/paragraph/5/enacted

- 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 which:

    - was provided by the data subject 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 data subject consented in the expectation that the information would not be so disclosed, or
    - which the data subject has expressly indicated should not be so disclosed

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

    - 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

  http://www.legislation.gov.uk/ukpga/2018/12/schedule/3/paragraph/21/enacted

- Disclosure would reveal information that is:

    - subject to a court order
      http://www.legislation.gov.uk/ukpga/2018/12/schedule/3/paragraph/3/enacted

    - subject to human fertilisation and embryology legislation
      http://www.legislation.gov.uk/ukpga/2018/12/schedule/4/paragraph/2/enacted

- subject to adoption legislation
  http://www.legislation.gov.uk/ukpga/2018/12/schedule/4/paragraph/3/enacted

- subject to special educational needs legislation
  http://www.legislation.gov.uk/ukpga/2018/12/schedule/4/paragraph/4/enacted

- subject to parental orders legislation
  http://www.legislation.gov.uk/ukpga/2018/12/schedule/4/paragraph/5/enacted

- The records refer to another individual who can be identified from that information (apart from a health professional). This is unless

  - that other individual's consent is obtained, or
  - the records can be anonymised, or
  - it is reasonable in all the circumstances to comply with the request without that individual's consent, taking into account any duty of confidentiality owed to the third party

  http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/3/enacted
  Article 15(4) of GDPR

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.

One example of this is an entry in a child's record: "*mum says father is drinking*".
This information *does not* contain data about the child.
This should be redacted when disclosing the notes to the father. It contains information *given by the mother about the father*. Although the information mentions the father, because it has been given by the mother it is deemed to be third party information in this context so it should be redacted.

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. Where there is any doubt as to whether disclosure would cause serious harm, the appropriate health professional should discuss the matter (anonymously, if needs be) with an experienced colleague, their Data Protection Officer, the Caldicott Guardian, or a defence body.

Guidance on redacting information within the medical record, in response to a SAR, is available
https://www.dropbox.com/s/t9a53eicjm9sx88/SARs%20brief%20guide%20for%20GPs.pdf

Access to Medical Records Act

The Practice will not provide information under a Subject Access Request 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 Records Act 1988. This would refer to reports for employment (proposed or actual) and insurance purposes (any "insurance contract" so covering 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 Practice will seek clarification from both the requestor and the patient concerned.

Informing of the decision not to disclose

If a decision is taken that the record should not be disclosed, a letter must be sent by recorded delivery to the patient or their representative stating that disclosure would be likely to cause serious harm to the physical or mental health of the patient, or to any other person. The general position is that the Practice should inform the patient if records are to be withheld on the above basis.

If, however, the appropriate health professional thinks that telling the patient:

- will effectively amount to divulging that information; or
- is likely to cause serious physical or mental harm to the patient or another individual

then the GP could decide not to inform the patient, in which case an explanatory note should be made in the file.

The decision can only be taken by the GP and an explanatory note should be made in the file. Although there is no right of appeal to such a decision, it is the Practice's policy to give a patient the opportunity to have their case investigated by invoking the complaints procedure. The patient must be informed in writing that every assistance will be offered to them if they wish to do this.

In addition, the patient may complain to the Information Commissioner for an independent ruling on whether non-disclosure is proper, 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 at the latest *within 1 calendar month*. This is calculated from the day the request is received.

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

OHG 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.

In addition to the information requested, the additional information that must also be provided (as per Articles 13 and 14) should be included by means of a link to the Practice GDPR Booklet and pointing out the relevant privacy notice (for GP records, this will be "EMIS Health Ltd – EMIS Web").

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 health record may be given to the patient 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 patient, then verifiable identification must be confirmed at the time of collection.

Holding the SAR safely at the surgery until the patient can collect it, or providing it by email or secure download, is the most secure way of supplying the record to the data subject. In doing so, we have implemented appropriate organisational and technical measures to ensure that:

- the information contained within the medical records remains confidential
- is accessed only by the individual to whom the data belongs, and not accidentally, or deliberately, accessed by someone else
- there is no accidental loss, destruction, or damage of the record in transit
- the medical record 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).

Providing the record for collection also meets the requirement to ensure that:

*"This right of access should be **easy**"*

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/how-can-i-access-my-personal-data-held-company-organisation_en

As of 1st January 2020, OHG's approach to providing SARs is as follows:

- On receipt of a SAR, whether directly from the data subject or a SAR made with the assistance of a 3rd party, the record will start to be prepared
- We will contact the data subject directly, offering them the option to receive their SAR in any format of their choosing

Data subjects, therefore, can be provided with their SAR:

- As an encrypted pdf by email; or
- As an encrypted pdf that they can securely download from Dr Neil Bhatia's Microsoft OneDrive account; or
- As an encrypted pdf on a USB drive; or
- As a printout

OHG will gradually move to providing *all* SARs electronically as the ideal.

However, we recognise that not everyone can receive and review an electronic SAR. Some individuals do not have PCs or may find access to a computer difficult (e.g., those patients who are homeless).

Confidential information should not be sent by email unless:

- the email address of the recipient is absolutely verified, and
- the information is sent *securely*; that is, encrypted (256bit AES) and the password conveyed *separately* (by SMS, in person, by telephone or by letter)

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

We may choose to provide the information in this way for any request, particularly very large SARs, but a USB stick must be new, purchased by the Practice, and the data *must* be encrypted. If the patient, however, wishes a printout of their record instead then we must supply it in that format.

All printed records will be left for collection in a secure bag.

If sent by post (in exceptional circumstances):

- the record should be sent to the named individual (data subject)
- by recorded delivery (Signed For™)
- marked "private and confidential"
- "for addressee only"
- and the Practice details should be written on the reverse of the envelope

The overwhelming majority of our patients live locally to the 3 sites 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).

Occasionally, the contents of a SAR might best be provided to the patient by hand-delivering the information. This is likely to apply where the patient is absolutely and genuinely housebound (e.g., the patient might be disabled or in a nursing home), and where alternative methods of provision (collection by a trusted third party, or securely posted) are neither suitable nor safe.

There are no circumstances where providing the information in a SAR by fax can be justified.

Disclosure to 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

https://www.lawsociety.org.uk/support-services/documents/bma-law-society-consent-form-oct-2018/

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 data subject access request (DSAR), and the request must be treated as such (no fee usually, response within 1 calendar month etc).

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. 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.

Oakley Health Group will look carefully at the particular circumstances of each request and assess that request discretely in its own context.

It would be wrong to have a blanket policy of *never* supplying third parties with a data subject's SAR.

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

- that the data subject would not in a position to be aware of, and verify, the lawfulness and nature of the processing of their personal data, in line with Article 63 of the GDPR

- that the data subject would not be in a position to exercise their right to object to aspects of processing of their personal data

- that 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

- that 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

- that 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

- that 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

- that, 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

- that failing to provide a copy of their 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

- that 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
- be allowing the data subject access to *their* personal data
- be 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
    - 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 "Your Data Matters" campaign (Appendix 2):

*"**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 patient (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.

The fact that the patient/data subject has capacity to *request* (or "authorise") disclosure of their SAR to a third party neither *obligate*s the surgery to do so nor sets aside the legal obligations under Article 15.

There are no provisions in Article 15 of GDPR, and no requirement 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.

There are no provisions in Article 15 of GDPR, and no requirement under data protection law, whereby a DSAR is lawfully fulfilled by bypassing the data subject and disclosing (i.e. *processing*) their personal data to a third party.

There are no provisions in Article 15 of GDPR, and no requirement under data protection law, whereby data subject rights are "transferred to" or "inherited by" a third party assisting a data subject in making the request.

Our patient – the data subject - does not, nor cannot, sign away, transfer, confer, delegate, or lend, their subject rights by virtue of the form of authority. Data subject rights cannot be subject to bailment.

There are no provisions in Article 15 of GDPR, and no requirement under data protection law, whereby a data controller-data subject relationship is generated between the GP surgery and the third party assisting an individual making a DSAR.

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 obligations as data controllers is to "supply", or "provide", the data subject (the requester) with the SAR (not "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
https://ico.org.uk/media/for-organisations/documents/2259722/subject-access-code-of-practice.pdf

"The data controller must provide ***the data subject*** *with a copy of the personal data being processed."*
Handbook on European data protection law 2018, EU FRA/CoE/EDPS

According to the Hessian SA, the 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 not only apply to *which* organisations receive, or have access to, a patient's personal confidential information, but 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."*

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/the-main-principles-of-this-guidance

Data retention policy

All SAR information – whether printed out or stored electronically – will be kept for a maximum of 18 months before being permanently destroyed/deleted.

Lloyd George records – currently scanned into a PDF file – will ideally be uploaded to the EMIS Web GP record (once checked and redacted, if necessary, by the GP). This process can also apply to individual documents. Such documents can be marked as redacted and disclosable (under a SAR) and/or visible via secure online access.

If appropriate, an *unredacted* copy of the PDF/document can also be uploaded if needed - for use by healthcare professionals *only* and not for disclosure under a SAR or available to the patient via secure online access. The document(s) should be marked as unredacted and non-disclosable.

Risk Analysis for Microsoft OneDrive

Oakley Health Group has undertaking an appropriate risk assessment for providing SARs via Microsoft OneDrive:

https://www.dropbox.com/s/c9fki6cux4m8yez/OneDriveRiskAssessment.pdf?dl=0

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 required 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.

Appendix 1 – Letter from OPG

Office of the Public Guardian
PO Box 16185
Birmingham B2 2WH

Tel: 0300 456 0300
Fax: 0870 739 4078
DX: 744240 (Birmingham 79)

OPGInformationAssurance@publicguardian.gov.uk
www.gov.uk/office-of-public-guardian

[redacted]

OPG ref: N/A

9 October 2019

Dear [redacted]

Re: Advice regarding LPA Property & Finance & request for medical records

Thank you for your **email** of **17 September 2019** in which you said:

"I would be very grateful for your advice: does the OPG regard an LPA for Property & Finance (alone) as granting an attorney authority (legal power) to access an individual's full GP medical records?"

My apologies for the delay in responding.

I can confirm the OPG does not regard an LPA for Property & Finance (alone) as granting an attorney authority to access an individual's full medical records.

OPG advice in this situation would be for the attorney to apply to the Court of Protection for specific authority to view the healthcare records in the best interests of the donor. This guidance is in line with the OPG's Code of Practice, Chapter 7 paragraph 56, which states:

"*A personal welfare attorney has no authority to make decisions about a donor's property and affairs (such as their finances). A property and affairs attorney has no authority in decisions about a donor's personal care. (But the same person could be appointed in separate LPAs to carry out both these roles.) Under any LPA, the attorney will have authority in a wide range of decisions. But if a donor includes restrictions in the LPA document, this will limit the attorney's authority (section 9(4)(b)). If the attorney thinks that they need greater powers,*

they can apply to the Court of Protection which may decide to give the attorney the authority required or alternatively to appoint the attorney as a deputy with the necessary powers."

You can read the Code of Practice at:
https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice

It should also be noted that even if a Health & Welfare LPA was in place, an attorney should only be asking for specific pieces of information relevant to the decision being made. A GP, for example, would be within their rights to deny blanket access. Again, this is covered in detail within the MCA Code of Practice, in Chapter 7, paragraph 23 which says: *"A personal welfare LPA can only be used at a time when the donor lacks capacity to make a specific welfare decision."*

I hope this clarifies the position but should you have any further questions please feel free to contact us by email on opginformationassurance@publicgaurdian.gov.uk

Yours sincerely,

[redacted]
Knowledge & Information Manager
Office of the Public Guardian

Please see this link for OPG's Personal Information Charter and Privacy Notice:
https://www.gov.uk/government/organisations/office-of-the-public-guardian/about/personal-information-charter#privacy-notices.

Appendix 2 – ICO "Your Data Matters"

Right of access

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. There are exceptions, but it's your right to ask if it's reasonable. In most instances, you should receive the information free of charge, and within one month. If your request is excessive, an organisation may charge a fee or refuse it, so it's best to make sure it's one you really need to make.

You're entitled to know:

1. Why your data was collected and how it was processed.
2. How long your data will be kept.
3. Who has seen or had access to your data.
4. Whether your data has been used to make an automated decision about you.
5. Whether your data has been used to create a profile about you.

Have you positively identified the patient? ☐	
Name of patient	
DOB	
NHS Number	
Date of request	
How was request made?	Face-to-face ☐ Telephone ☐
	Does the patient want secure online GP records access? ☐
	Does the patient want a copy of "*their entire GP record*"? ☐
Details of request	If not the entire record, then what exactly? e.g. records between two dates, records about a medical condition, only hospital letters, etc.
How does patient want the information to be provided?	By secure download ☐ By email ☐ On a USB drive ☐ Printed ☐ Other (specify) ☐
Remind patient that he/she might be contacted by the practice for further information or clarification about the request, if needed	
Pass this request on to the Practice Manager or the Information Governance Lead	

Subject Access Request

Oakley Health Group

I would like to make a Subject Access Request for my personal information.	
Name of patient	
DOB	
NHS Number (if known)	
Date of request	
	Do you want secure online access to your full electronic GP record? This might easily provide you with all the information you seek, 24hrs a day, as well as the ability to make appointments and request medication. Ask at reception or visit our website.
	Do you want a copy of your *entire* GP record? ☐
Details of request	If not your entire GP record, then please detail exactly what information you would like. For example, between two dates, or relating to a particular medical condition, or hospital letters only.
How do you want the information to be provided?	By secure download ☐ By email ☐ On a USB drive ☐ Printed ☐ Other ☐ (specify)
Please note that you might be contacted by the practice for further information, or clarification about the request, if needed. Any questions? Contact our Data Protection Officer.	