Dear

Title Given Name Surname
Your Ref:

Further to your letter dated *****, we have now prepared the relevant Data Subject Access Request information as requested.

- We have provided them with their GP record, directly, as an encrypted pdf via email/on a CD/on a USB drive/as a printout, as requested by the data subject
- We have offered to supply them with the requested record in any other format, as an alternative (i.e. via email/on a CD/on a USB drive/printed)
- They have been provided with your email address and your telephone number, should they choose to forward the SAR to you in this way
- We have also provided them with your postal address, should they decide to send some or all of the record to you in this way
- We have provided them with your reference number
- They have been provided with the password for the encrypted record
- They have been reminded to provide *you* with any such password *separately* (e.g. by telephone or an alternative email address)

Disclosing the SAR directly to a third party would neither:

- be providing the data subject with a copy of their personal data, nor
- be supplying the data subject with a copy of their personal data, nor
- be sending the data subject a copy of their personal data, nor
- be allowing the data subject access to their personal data, nor
- be enabling the data subject to be aware of, and verify, the lawfulness and nature of the processing of their personal data, nor
- be enabling the data subject to exercise their right to object to aspects of processing of their personal data, nor
- be enabling the data subject to determine the accuracy of their GP medical record (incorrect or missing diagnoses) and, if so needed, exercise their right to rectification, nor
- be enabling the data subject 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, nor
- 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
- nor be upholding the data subject's right of access in any way

which would be a contravention, by us, of Article 15 and the principles of Recital 63 of the GDPR.

We have dealt with this request as if the patient had made the request directly (and out with your assistance) and have disclosed the information accordingly, in line with Article 15 and any pre-action protocol as might be required by a court.

We assessed the data subject's request as neither manifestly unfounded, nor excessive, nor unduly complex – and as such it was accepted, processed, and provided/supplied free of charge in line with Article 12.

We have fully responded and cooperated with their request and have enabled the data subject to exercise their information rights (Articles 16, 18 and 21).

We have also offered the data subject to register with the surgery for secure online access to their full electronic GP record, enabling them to look at and/or download their GP record – in particular, any *future* information added to their record - whenever they like, and without the need of making a further subject access request.

We therefore have fulfilled our legal obligation to the data subject and met the legal standards of Article 15 and Recital 63 of the GDPR.

We have also upheld the General Medical Council's principles of confidentiality, namely:

- (b) *Manage and protect information*. Make sure any personal information you hold or control is effectively protected at all times against improper access, disclosure or loss
- (d) *Comply with the law*. Be satisfied that you are handling personal information lawfully
- (h) *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

We have also upheld The National Data Guardian's second guiding principle, namely:

- There should be *no surprises* to citizens and they should have choice about the use of their data

We are mandated to provide the data subject with their SAR. We are not mandated to transfer, or disclose, personal confidential medication information to a third party either:

- as a result of a data subject's access request, and/or
- as a result of our patient having the capacity to request disclosure of their SAR directly to a third party

There are no provisions in Article 15 of the GDPR that compel us to process data in that way.

There are no provisions in Article 9 of the Council of Europe's Convention 108+ (for the protection of individuals with regard to the processing of personal data) that compel us to process data in that way.

There are no provisions in Article 15 of the GDPR, or in Article 9 of Convention 108+, whereby:

- a DSAR is lawfully fulfilled by bypassing the data subject and disclosing (i.e. processing) their personal confidential information to a third party
- a third party becomes a data subject, or "inherits" data subject rights, by virtue of assisting the individual in making their DSAR
- a data controller-data subject relationship is generated between the GP surgery and the third party assisting an individual making a DSAR

An organisation cannot be, or "become", a data subject because a data subject must be 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" (Data Protection Act 2018, Part 1 3(5)).

Our patient – the data subject - does not, nor cannot, "sign away", "transfer", or "lend", their subject rights by virtue of the form of authority. Neither does the form of authority set aside our legal obligations to the data subject under Article 15.

In addition, Recital 63 of the GDPR encourages controllers, where possible, "to provide remote access to a secure system which would provide *the data subject* with direct access to his or her personal data". We are under no obligation to provide third parties with such access.

We attach a factsheet for information, and which further explains our process for complying with Subject Access Requests in such circumstances. Please note that we have offered you a lawful and established way of receiving medical information from the data subject's GP record *directly*, out with a data subject access request.

Holding the SAR safely at the surgery until our patient can collect it (or emailing an encrypted version of the SAR to the patient) 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
- the record 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

Whilst the data subject is now at liberty to arrange transfer of some or all of the medical record that they will hold to you, if they so choose to, we have reminded them to always hold a *full and unamended* copy of the SAR so that, for example, they are in a position to comply with a court directive for such disclosure.

Kind regards,

Subject Access Requests – a guide for third parties

Where is the SAR?	The SAR has been provided *directly to the data subject (our patient)*.
What has changed?	The introduction of GDPR and the Data Protection Act 2018 require data controllers to *clearly* facilitate and uphold data subject rights – including the right of access, and subsequent to that: the right to rectification, the right to object, and the right to complain to a supervisory authority if warranted
Is releasing the SAR "processing personal data"?	Disclosing the SAR information *directly to the data subject* is a legal obligation under Article 15 of the GDPR – it is a *data subject right*. Disclosing the requested information, with or without the data subject's consent (or form of authority), to a third party *is processing* of personal data. It would be the transfer of confidential medical information from one data controller (the GP surgery) to another data controller (a third party). Such disclosure to a third party is *not* a legal obligation.
Would the data subject know what information is likely to be in the SAR?	The data subject cannot possibly know or understand, until he/she has seen it in its entirety, what information is in their SAR. If the entire GP record, or a very significant part of it, has been requested, it will contain a large amount of very sensitive information that may have no bearing whatsoever on the purpose of the SAR. Patients, in our experience, do not appreciate the sheer volume and detail contained within what is arguably the most comprehensive, cradle-to-grave, electronic primary care medical record anywhere in the world. The data subject has full capacity to receive and understand the SAR and make appropriate decisions on further sharing of that information with third parties. The data subject has total control over the record, as is their right.
Have we charged for providing the data subject with the SAR?	No. Neither the data subject nor the third party making the SAR on behalf of our patient has been charged a penny, in line with Article 12(5) of the GDPR. By providing the SAR directly to our patient, we ensure that they are able to make as many copies of their information as they like, before deciding whether to disclose any or all of the information to a third party, so making any repeat requests for their information from us - and for which we are entitled to charge a fee - unnecessary.
To whom has the SAR been provided?	We have disclosed the SAR (in whatever format) directly to the data subject. We have provided/supplied the record as required. We (the data controller) are not mandated to release the contents of a SAR *to anyone else but the data subject*, irrespective of the data subject's "wishes". GP surgeries do not take "instructions" from patients..
How have we provided the SAR to our patient?	The SAR has been made available for collection, in person and with suitable ID, at any of our surgery sites. Patients collect all other forms, letters, certificates, sick notes, or directly made SARs, that we provide them with. Our obligation is to *provide* the data subject with the SAR, and it is their right to *obtain* it from us. The data subject is perfectly capable of collecting the SAR from the surgery (as far as we know). Alternatively, we may have emailed the data subject their SAR. We are under no obligation to post, fax, courier, or deliver in any other way, the printed SAR to the individual's home (or other address). It is a right *of access to* information, not a right *to be posted* information.
What about data subject rights?	A SAR is the *data subject* right, not a *third party* right. It is a *data subject* access request, not a *third-party* access request.
What about s184 and s185 of the DPA 2018?	Sections 184 and 185 of the DPA 2018 afford the data subject important protections and safeguards for their confidential medical information which would be bypassed, to his/her detriment, were we to disclose their SAR directly to a third party. It is not a criminal offence for a data controller to disclose a SAR to a data subject if it is believed, or suspected, that it could be an "enforced" SAR. It becomes a criminal offence when a third party asks, "invites", "requests", requires, compels, or coerces an individual to disclose the information so provided, to that third party, in relation to a contract for services or the provision of services. In addition, to require an individual to exercise their subject access rights and to supply their heath records will render a term or condition of contract as void.

What does the ICO say about data controllers and "enforced" SARs?	The ICO states that: "*If you have received the enforced SAR, you should be providing the information to the individual who has the right to receive such information*".
Has the SAR been amended or altered in any way?	We have disclosed the requested GP record to the data subject, suitably redacted to ensure that any information so released: • Does not disclose anything that is the personal data of any other individual (third party), unless that information was supplied directly by the data subject • 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
A SAR is not….?	• A SAR is not designed to allow third parties to obtain personal data that the data subject does not, or *might* not, want disclosed. • A SAR is not (and was never intended to be) the mechanism for the provision of medical records, for legal purposes, that can be relied upon to be unaltered or unamended (i.e. as a "chain of evidence").
Who has control….?	The data subject (as a party) has control of the record and can disclose that information as wished, or as ordered by the court.
What is your role?	As an authorised third-party, you have facilitated the *data subject* making *their* subject access request. And it remains *their* request (not yours), for *their* personal confidential data.

How can third parties lawfully receive information for legal purposes?	The GDPR has an entirely separate and standalone lawful basis – a clear and established legal route, and the correct legal framework - for processing health (special category) data to support the investigation, preparation and pursuit of legal claims, in the form of Article 9(2)(f).
	
	This would be a medical report, *not a SAR*. A medical report of this nature is a long-established service that GP surgeries provide out with their NHS contract.
	
	We would:
	
	• charge a reasonable fee for such work - *as we are entitled to do*
	• require a simple *form of authority*:
	  ○ providing explicit permission from the data subject; and
	  ○ defining the *relevant* medical information sought (which *might* be the entire record, if appropriate and necessary)
	• aim to provide you with the report within 40 days
	• retrieve the information
	• identify *any possibly relevant* information
	• exclude information that *was not possibly relevant* to the claim
	• check it for accuracy
	• redact any third-party information, if needed
	• not be disclosing the entire medical record to you (unless justified)
	• not be providing you with any medical opinions
	• be providing you only with factual extracts from their medical record
	• enable the data subject to view the information *first* (if he/she so wishes)
	• then securely provide you with the prepared records