# (revised 1st May 2018)

# 7 Blog Seven Subject Access Requests, SARs and TSARs

**What’s different about Subject Access Requests (SARs)?**

The fundamental has not changed, its their data, they must have access to it. So, whilst there might seem to be many reasons for not giving up their data listed in this blog the default assumption remains that patients have a right to see their records and as DCs we should normally provide them access to it.

**Several things have changed regarding SARs.**

1. Firstly, you will not be able to routinely charge for copies of the DS’s records. You can charge, but not routinely, see later.
2. Secondly the data you must supply is more than just a copy of the data you hold, additional information (in effect the content of the relevant Privacy Notice) must be provided.
3. Thirdly any response to a SARs, see 4 below, must now be within “one month” (no longer 41 days and the definition of the “one month” varies[4](#four), I’d advise assuming a blanket 28 days response deadline).
4. Fourthly, there are new potential responses to a SAR which include; 1) you can agree (the norm and not new) or 2) decline (not new, not advised and you’ll need to justify refusing) or 3) you can agree to respond but require more time (up to a max of two of those months, and you’ll have to explain why) or 4) you can negotiate (this is new!).

**So what’s the additional data we must supply?**

The additional information that you must supply, along with the copy of the original personal data concerning the DS, is listed in Articles 13 and 14 and is;

* The purpose(s) of the processing
* The categories of personal data being processed
* The recipients or categories of recipients
* The envisages retention period or the criteria that determine it
* The rights of rectification, restriction, objection and where applicable erasure.
* The right to complain to the ICO
* The right to know more about the source if not the DS
* The existence of and logic behind and consequences of any automated processing

Remember this, or an easily accessible link to it, has to be provided as well as the actual data relating to the DS. I’m going to call these Additional Processing Information notices. Think of them as a cover page or frontispiece for all SARs.

**1) You can agree (to the full SAR).**

If you agree to the SAR must respond within one month and include all the data you hold on the DS plus whichever of the information listed above that applies. Providing copies of all the data you hold is the norm.

**2) You can decline**

You can decline, or as GDPR puts it; “not take action” to provide a SAR. This is not at all advised and you’ll have to justify why and provide the justification within the universal one-month deadline and explain how the DS can complain against your decision. One obvious reason for declining is if the data has not changed since a previous request.

**3) You can agree to respond but require more time**

You can agree to supply the data, all the data plus the additional information, but because of the difficulties of collating and supplying the data you (and you alone) can decide you need more time. You can have up to an additional two months. If you decide you need the additional time you must let the DS know within the universal response one-month deadline. This will also apply to the SAR variants. The decision to seek more time is yours and yours alone, no one can challenge it.

**We’ve been collecting paper records since the 1940s and electronic stuff for 20 yrs., we now have masses of data on our patients, do we have to produce it all?**

**4) No, you can negotiate!**

This is the new one, a negotiated disclosure. Under GDPR (see Recital 63[1](#one)) it is possible to agree with the patient that only certain parts of the record are produced under a SAR. A SAR was defined under DPA as the entire contents of the patient record and under GDPR whilst that is the same basic default assumption it’s been recognised that 20 or more years later we hold masses of data on our patients, so a new option has been introduced; a SAR can now be less than the entire record by mutual agreement, I shall call these a “Targeted SAR” (TSAR).

**Tell me more about TSARs**

GDPR allows the DC to ask the individual to specify the information the request relates to, which could narrow down the data needed to satisfy the request. The absolute proviso is that the DS must agree and do so voluntarily and freely. You can’t use a TSAR to coerce people into asking for less than they want or need. In these circumstances it would be best to clearly document what is agreed as being the scope of the first TSAR, for instance; only the records of a hip operation. Agreeing with the DS what is going to be covered by the SAR must occur within the “one month” timeframe above.

**What else could be a TSAR?**

Some might say a negotiated TSAR is going to be more difficult and time consuming than just unloading the lot, but remember GDPR applies to all data formats; it includes the paper in the Lloyd George envelopes. So, a sensible TSAR might be everything you have on the DS in electronic form. I can imagine in most circumstances the patient is not likely to want copies of the irrelevant historic paper records. Another might be a simple everything from a certain date. There are other options and I’ve asked the suppliers to facilitate making these easier to action. Remember even for the laziest “download everything SAR” you still have to protect any other DSs mentioned in the requestor’s records, i.e. redaction of non-medical 3rd parties. The less there is to hand over, the less there is to redact.

**And about all disclosures, electronic by default**

“Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form”. Furthermore Recital 63 provide us GPs with a very useful steer; “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”. So that looks like Patient On-Line access would fit that bill very nicely. Signing patients up for NHS provided On-Line Access[3](#three) and ensuring they have a link to your PPN or PNs would satisfy GDPR DS access rights in full.

**When can I charge?**

There is a developing myth that you cannot charge for SARs or TSARs. This is a myth, doubly so, because there are in fact two conditions under which you can charge, one, for straightforward copies and two, for burdensome, irksome, vexatious and irritating requests. And the charges allowed are also different. So note this section carefully, its taken me two attempts to get it right!

**One, straightforward copies, (Article 12, para. 3)**

The clause says it all, plain and simple, black and white, first one is free, copies are not. “The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.”[2](#two).

Please post those words “administrative costs” in a mental siding because we’ll come back to them later.

Back to copying, GDPR makes no comment on how long it is before a repeat is no longer a copy.

**Meaning?**

Medical records can potentially be added to every day, certainly the contents of many patients’ records will have changed in 6 months time, so is a request for another SAR 3 months after a previous likely to be a copy or a new SAR?

I would argue it depends on content. If the data being handed over to the DS is essentially unchanged, even if its years later, it’s still a copy. And thus chargeable.

**Two, irksome, vexatious or irritating requests, (Article 12, para. 5)**

The other chargeable circumstance arises from Article 12, para (5) which reads;

5.   Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

|  |  |
| --- | --- |
| (a) | charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or |

|  |  |
| --- | --- |
| (b) | refuse to act on the request. |

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Now that paragraph is a construct of an opening sentence saying no charge which then ends abruptly. Its followed by a second sentence that starts “Where…”. There’s a full stop between them and no direct link. And if there’s no linkage someone somewhere will try to exploit it, getting everything for free. Setting aside the fact the second sentence is clearly intended to qualify the first,

**Can we find a more explicit link that can’t be disputed?**

Oh yes we can. The wording from the [official guidance](https://www.dropbox.com/s/pwbbpq19uch29e6/Official%20GDPR%20Guidance%20on%20Portability.pdf?dl=0) reads; “Article 12 prohibits the data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, “in particular because of their repetitive character”.”

The wording of the official guidance brings together the “first free” element of para. 3) and merges it with the para. 5), irksome and irritating. The wording makes it plain any excessive or unfounded SAR can be charged for. Full stop, period, end off, job done.

Any excessive or unfounded request, even if it’s a first request.

**To summarise**

GDPR allows DCs to charge for copies of previously provided SARs or TSARs and any that are unfounded or excessive, and if they are judged to be unfounded or excessive, you can charge for even the first request, let alone copies (surely copies of unfounded and excessive would attract a healthy premium!).

**Statement: It is not true that you cannot ever charge for a SAR or TSAR.**

**But it gets better, 5 charges for unfounded or excessive requests under para. 5) are more flexible than the para 3) “administrative costs”**

Article 12(5) offers GPs several options. They can comply with the request, produce the report but charge for the inconvenience (Article 12(5)(a). If you decide to comply with the request, you may then charge for either;

1. ”the administrative costs”

or

2) “providing the information”

or

3) “communicating the data”

or

4) “taking the action requested.”

|  |  |
| --- | --- |
|  |  |

So, the fee under 4) above might involve the cost of professional time to redact records, for example.

**Alternatively**

Article 12(5)(b) allows the GP to simply refuse to comply with manifestly unfounded or excessive requests.

**The DC shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.**

Neither “unfounded” nor “excessive” are defined in the GDPR nor its guidance so interpretation is going to have to be an application of the reasonableness factor. GDPR does provide some clue in describing “repetitive character” as being a qualifying criterion for excess.

**And it won’t only be hard nosed ambulance chasers**

We once had a patient with 17 Lloyd George envelopes that weighed in excess of 12 kg. I can see that even a simple plain honest request for copies of those records could be argued to be excessive, in other words chargeable. This would not be against a background of complaint, investigation or dissatisfaction, it might be your sweetest most favourite patient simply wanting copies of all their records, but nonetheless the work involved in copying and redacting the 2,100 pages in those 17 envelopes should certainly be recompensed.

**But bear in mind**

If you invoke anything under Article 14(5), either declining or complying but with a charge you must be able to justify your actions.

**OK so how’s this going to work in practice?**

We redact and then copy the 17 Lloyd George envelopes, we put them in lever arch files, stack them in storage boxes and then say come and get them, there’s a bill for £500 to pay. Guess what, they change their minds and no longer want them. You’ve now got 24 kg, 4,200 pages of notes and have lost 2 days staff time.

My advice, if you are contemplating a charge, is to get the charge at least agreed with the DS before you do the work. Even better would be paid in advance.

I have seen nothing in GDPR that says you cannot adopt this approach.

**What about 3rd parties acting for the DS?**

You cannot ordinarily charge for a SAR or TSAR. It makes no difference who it is being delivered to. The DS must have access, directly or indirectly, to the first SAR or TSAR free of charge. If you hand it over to their nominated 3rd party for free then you have provided access free to the DS because the nominated 3rd party is the DS by proxy and you have complied with GDPR. You cannot charge a 3rd party intermediary who represents the DS for a SAR or TSAR.

**Can I provide a SAR orally?**

Yes, you know it’s the patient; you can action the SAR there and then. Obviously, this is likely to be a TSAR. And I can conceive of no circumstance of your being able to charge, unless you did a sort of talking book extended reading.

**Saying No a SAR or TSAR?**

If you refuse a request it will be important to document your reasons for doing so and you must communicate them to the DS within the same one-month response deadline. If you do decline a request, you must let the DS know their rights to complain about your decision to the ICO and it would be wise to also refer to your DPO.

**Other GDPR exceptions**

In relation data gathered from the DS themselves, i.e. data they provided, or you got from them directly, there is an exception to providing copies “where and insofar as, the data subject already has the information”. So if they gave you a spreadsheet of BPs, you don’t need to be able to give them a copy back. Please note this applies to both the personal and special category data relating to the DS as well as the additional data mentioned in [2](#additional) above.

In relation to data gathered from elsewhere, i.e. other than from the DS themselves, which is a lot in medicine, think OPD letters, discharge summaries etc, other exceptions for providing data can apply. They are; firstly, the manifestly obvious “they’ve already got it” reason (Article 14.5(a)). Think letters copied to patients scheme.

Articles 14.5(b)(c) and (d) allow for the other exceptions;

Article 14(5)(b), “The provision of such information is impossible or would involve a disproportionate effort or would make the achievement of the objectives of the processing impossible or seriously impair them.”

**Impossible?**

One would imagine most incoming data about our patients’ identified both them and the source, so this is unlikely to ever apply for GPs.

**Disproportionate effort?**

If a patient has hundreds of hospital letters or thousands of test results, it might be reasonable to argue that the letters from the 1960’s are probably no longer relevant. GDPR states that accessing old and aged data from obsolete or hard to access filing systems could be deemed to require disproportionate effort.

**Make impossible or seriously impair?**

Neither of these is likely to be available for a GP.

# Article 14(5)(c), “The data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject’s legitimate interests”

**Law**

This is where a law requires a DC to collect data on DSs from elsewhere. In that circumstance the DC is not bound to disclose that data to the DS. I cannot think of any circumstance where this will apply to GPs and their patients. Possibly safeguarding?

# Article 14(5)(d), “An obligation of professional secrecy (including a statutory obligation of secrecy) which is regulated by national or EU law means the personal data must remain confidential”.

**Professional secrecy**

This is what GPs can rely on; it’s essentially the same as redacting 3rd party information. You wouldn’t disclose comments about a 3rd party to the DS, the exception to this exception being the identity of others involved in the care of the patient.

**Other general exceptions**

And remember these other more generic exceptions;

You shouldn’t disclose anything that identifies any other DS. The only exception to this is the identity of people involved in the care of the DS, such as community staff or hospital specialists, they are not exempt.

You mustn’t disclose anything that is likely to result in harm to the DS or anyone else.

You mustn’t disclose anything subject to a court order or that is privileged or subject to fertilisation or adoption legislation.

**Do I have to provide SARs on USB sticks or CDs?**

No. You can agree the medium with the DS. GDPR and the ICO are very much in favour of electronic SARs and TSARs. If the SAR or TSAR request is made electronically it is expected that the response will be provided electronically. Copies, unfounded or excessive records could be provide on fobs, CDs or cards but these would all be chargeable.

**Under the DPA insurers tried to get around the Access to Medical Records Act by getting patients to “request” SARs which were then forwarded to the insurer. Why won’t they use this new “modified SAR” option to do the same again?**

Because clause 181 of the Data Protection Bill will extend the offence of “enforced subject access”, i.e. where a patient is being coerced or tricked into providing a SAR derived copy of their records to support an application, to include medical records. This now becomes a criminal offence. Insurers will not want to be found guilty of the crime of enforced subject access. If any GP suspects that an insurer is doing this, they should report them to the ICO and the ABI. As a reminder the [ABI](https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2017/health/requesting-and-obtaining-medical-information-electronically.pdf)  and the [BMA](https://www.bma.org.uk/-/media/files/pdfs/practical%20advice%20at%20work/doctors%20as%20managers/managing%20your%20services/focus%20on%20subject%20access%20requests%20for%20insurance%20purposes%20august%202015%20full.pdf?la=en) have issued guidance previously and this is unchanged under GDPR.

**So what happens when we get a solicitor’s letter?**

Depends what it says and what its asking for. If its unclear seek clarification.

**Can a solicitor ask for a SAR or TSAR?**

Yes, third parties and legal representatives can ask for SARs and TSARs on behalf of the DS. What they cannot do is seek a SAR or TSAR to support an application that should be made under the Access to Medical Reports Act.

**How do I tell the difference?**

The Access to Medical Reports Act (AMRA) deals specifically with reports for employment and insurance purposes. Note the insurance purposes is not just life insurance and mortgages, its any “insurance contract”, so it covers accident claims, insured negligence, anything covered by an insurance contract that requires a medical report.

**But hang on, they could argue that a TSAR is the same as a report on a specific injury, like a whiplash?**

Correct, and no doubt some will try. However it is the purpose that determines the legal basis. If the solicitor’s letter does not make the precise purpose of the request and report clear, then ask them is the report being requested under GDPR or AMRA? If the report is to support an actual or potential insured claim then AMRA applies. You can charge and no APIn is needed.

**And employers?**

The same distinction applies. If the report is in connection with proposed or actual employment, its not a SAR or TSAR and you can charge and no APIn is needed.

**Quick fire action points**

1. Revise your SAR request procedures and paperwork
2. Create an Additional Processing Information notice (APIn)
3. Provide a copy of, or link to, the APIn with every SAR or TSAR
4. Utilise the new response options, particularly the TSARs
5. Be aware (wary?) of the tighter deadlines
6. Be very wary of solicitor’s and others’ letters. Be prepared to clarify requests.
7. Anything to do with insurance or employment, its not GDPR.

# Dr Paul Cundy

# GPC IT Policy Lead

# GMC 2582641

# 12th April 2018

1, Recital 63, “Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.”

2, GDPR Article 15(3) “The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.”

3, <https://www.england.nhs.uk/patient-online/about-the-prog/po-gp/>

4, [Blog Twelve Q. How long is a month](https://www.dropbox.com/s/g5363lfpb36apyk/12%20Blog%20Twelve%20Q.%20How%20long%20is%20a%20month.doc?dl=0)