

RIGHTS OF ACCESS REQUESTS (SAR’s)

March 2021

Kelly-Anne Gast DPO ALMC

Rights of Access Request Process Map

|  |
| --- |
| PATIENT -SAR CONFIRMATION LETTER  TEMPLATE  19 March 2021  Our Ref: -XXX-XX-XXX  Private & Confidential  Recipient Name  Recipient Organisation  Address Line 1  Address Line 2  Address Line 3  Address Line 4  Dear Recipient Name,    RE: Subject Access Request  We refer to your personal data subject access request (SAR) made under UK Data Protection Law General Data Protection Regulation 2016 (GDPR) & Data Protection Act 2018. We received your request on Date and we have up to one month from receipt of your request in which to respond, i.e., until Date.  This time limit is calculated from the day we receive your request until the corresponding calendar date in the next month. If this is not possible because the following month is shorter and there is no corresponding calendar date, the date for response is the last day of the following month. If the corresponding date falls on a weekend or public holiday, we have until the next working day to respond.  We refer to your request dated Date in which you requested the following information:   * insert document requested * insert document requested * insert document requested * insert document requested * insert document requested   We will undertake a search of our systems and believe that we will identify a substantial amount of correspondence and documents that, whilst it may not fall within the scope of your request, will take some time to collate, review and put through the redaction process (if necessary) before we can release to you, as we are required to ensure that the data supplied only relates to you and not any third parties as you are only entitled to receive your own information that relates directly to you.  In the meantime, the GDPR requires us to provide you with further information in relation to the personal data within the scope of your request. Please see the Privacy Notice attached to this letter which sets out:   * Categories of personal data * Source of the personal data * Purpose(s) for processing in respect of each category * Legal basis for processing in respect of each category * Retention period (or basis for calculating such period) in respect of each category * Categories of recipients in respect of each category   As a data subject, you have a number of additional rights in relation to your personal data. Subject to certain conditions, and in certain circumstances, you also have the right to:   * request rectification of your personal data – this enables you to have any inaccurate or incomplete personal data we hold about you corrected * request the erasure of your personal data – this enables you to ask us to delete or remove your personal data where there’s no compelling reason for their continued processing, e.g., it’s no longer necessary in relation to the purpose for which they were originally collected * restrict the processing of your personal data – this enables you to ask us to suspend the processing of your personal data, e.g., if you contest their accuracy and so want us to verify their accuracy * object to the processing of your personal data – this enables you to ask us to stop processing your personal data where we are relying on the legitimate interests of the business as our legal basis for processing and there is something relating to your particular situation which makes you decide to object to processing on this ground.   If you wish to exercise any of these rights, please contact our Data Protection Officer (insert their name and contact details, including email address, telephone number and postal address) or complete the electronic form on the Organisation’s website.  Further information regarding your rights can be found at [www.ico.org.uk/your-data-matters/](http://www.ico.org.uk/your-data-matters/)  Yours Sincerely  Name  Job Title  🕿 CONTACT NUMBER  🖰 EMAIL ADDRESS |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PATIENT-SAR RESPONSE TEMPLATE  19 March 2021  Our ref: -XXX-XX-XXX  Private & Confidential  Recipient Name  Recipient Organisation  Address Line 1  Address Line 2  Address Line 3  Address Line 4  RE: Subject Access Request  We refer to your personal data subject access request (SAR) made under UK Data Protection Law GDPR 2016 & Data Protection Act 2018. We received your request on Date and we have up to one month from receipt of your request in which to respond, i.e., until Date.  This time limit is calculated from the day we receive your request until the corresponding calendar date in the next month. If this is not possible because the following month is shorter and there is no corresponding calendar date, the date for response is the last day of the following month. If the corresponding date falls on a weekend or public holiday, we have until the next working day to respond.  I can now confirm in response to your request as follows:   1. Your personal data is \ is not being processed by or on behalf of …. Practice Name 2. Your personal data being processed is as follows: (list categories of personal data) 3. The purposes for which your personal data is being processed are: (specify purposes for which personal data are being processed). 4. Where your personal data has not been collected from you, the source(s) of your personal data [is/are]: (insert any available information as to the source(s) of personal data) 5. Your personal information is shared internally within the Organisation, including with members of the HR department, members of the recruitment team, payroll staff, your line manager, other managers in the department in which you work (or applied to work) and IT staff if access to your personal information is necessary for the performance of their roles. The Organisation also shares your personal information with third-party service providers (and their designated agents). The recipients, or categories of recipients, to whom your personal data have been or will be disclosed are: (list the recipients, or categories of recipients, to whom the personal data have been or will be disclosed) 6. The envisaged period(s) for which your personal data will be stored [is/are]: (set out retention periods) 7. We do not transfer your personal data to third countries or international organisations. 8. We do not make any employment decisions about you based solely on automated decision-making, including profiling.   As a data subject, you have a number of additional rights in relation to your personal data. Subject to certain conditions, and in certain circumstances, you have the right to:   * request rectification of your personal data – this enables you to have any inaccurate or incomplete personal data we hold about you corrected * request the erasure of your personal data – this enables you to ask us to delete or remove your personal data where there’s no compelling reason for their continued processing, e.g. it’s no longer necessary in relation to the purpose for which they were originally collected * restrict the processing of your personal data – this enables you to ask us to suspend the processing of your personal data, e.g. if you contest their accuracy and so want us to verify their accuracy * object to the processing of your personal data – this enables you to ask us to stop processing your personal data where we are relying on the legitimate interests of the business as our legal basis for processing and there is something relating to your particular situation which makes you decide to object to processing on this ground.   If you wish to exercise any of these rights, please contact our Data Protection Officer Kelly-Anne Gast [kelly@almc.co.uk](mailto:kelly@almc.co.uk) or complete the electronic form on the Organisation’s website.  If you believe that the Organisation has not complied with your data protection rights, you have the right to make a complaint to the Information Commissioner’s Office (ICO) at any time. The ICO can be contacted on 0303 123 1113 (local rate) or via the Information Commissioner’s Office (ICO) website: <https://ico.org.uk/>  We confirm that we have carried out a reasonable and proportionate search to locate the personal data that you requested in your SAR and we now attach copies of some of the personal data requested in the following format: insert information on format, bearing in mind that where the data subject made their request by electronic means, you must provide the information in a commonly used electronic format, unless they request otherwise.  The personal data attached is indexed as follows:   |  |  |  | | --- | --- | --- | | Document Number | Description of Document | Date of Document | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  |   Please note that, as some of the information you requested includes personal data relating to third parties, we have redacted all information relating to third parties in order to protect their identities. Sometimes this could be whole pages of documents.  We have withheld some of the information you requested in reliance on a statutory exemption. Those types of documents are *(insert a brief description of the type of document involved)* and the particular exemption from disclosure that we are relying on is *(specify the exemption that applies, e.g. data covered by legal professional privilege, data processed for the purposes of management forecasting or management planning, material relating to negotiations and confidential employment references)*  This now completes our response to your Rights of Access request.  Yours Sincerely  Name  Job Title  🕿 CONTACT NUMBER  🖰 EMAIL ADDRESS  Did you know?  If you’re using a computer to redact information, make sure you get advice on how to save it as a new file. Otherwise, there’s a risk that someone could delete your blacked-out sections and read the text underneath.  [This Photo](https://commons.wikimedia.org/wiki/File:US_Navy_041019-N-5821P-019_Airman_Lauren_Thurgood_of_Las_Vegas,_Nev.,_pulls_patient_medical_records_in_the_inpatient_ward_aboard_the_conventionally_powered_aircraft_carrier_USS_Kitty_Hawk.jpg) by Unknown Author is licensed under [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/) |
|  |

# Did you know?

|  |
| --- |
| It doesn’t matter if the day you receive the request isn’t a working day. For example, if you receive a request on Saturday 7 March, you should respond by Tuesday 7 April.  [This Photo](https://theodi.org/article/explainer-what-is-personal-data-and-how-can-i-control-how-is-it-shared/) by Unknown Author is licensed under [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/) |
| ICO NEWS UK GP PRACTICE FINED!!!: Lessons to learn from a £40,000 fine for a mishandled subject access request. (BEFORE GDPR FINES NOW 2-4% OF GLOBAL TURNOVER) The UK’s privacy regulator, the Information Commissioner’s Office (**“ICO”**), has issued a GP practice with a fine of £40,000 for unlawfully disclosing the personal data of two individuals in  response to a data subject access request (**“SAR”**) from a third person.  In its public statement on the enforcement action, the ICO criticised the practice for not having adequate systems or training in place to ensure that its staff were equipped to deal with SARs properly. |

Patient Rights of Access Requests 2021

In order to comply with Data Protection Law on these requests we need to ensure all practices are complying with the following: -

Internal Procedures

### Be clear and transparent -We need to inform our patients ‘Data Subjects’ of their right to request their medical information if they wish.

### How do we achieve this? -

### This information should be provided within Privacy Notices, easily accessible via practice websites and there should be a dedicated email for these requests to filter through to avoid inappropriate sharing.

1. We need to ensure that every practice has a ‘Rights of Access’ Request Policy too which specifies internal procedures for any members of staff dealing with these requests. These should all include:

* Who is responsible for dealing with these requests?
* How to recognise these requests and how to handle them
* Timings and how this is monitored in order to ensure they are dealt with in a timely and efficient manner.
* Timeline of the procedure, or templates
* Redactions
* Information about Right to Rectification and Right to Erasure and Restriction of processing data.
* Exemptions that might apply

1. Ensure that the data is easily accessible to ensure a timely response, we have 30 days only in which to respond.
2. Ensure that the request is returned in the manner in which it was received, unless this is an impossible task, confirm with the data subject ‘patient’ to ensure they are happy with the method in which you intend to respond.
3. Keep a record of all requests, should include, how you responded and when you responded.

Are you currently doing this Yes or No?

RECEIVING A ‘RIGHTS OF ACCESS REQUEST’

Upon receipt

1. **Verify the identity of the Patient ‘Data Subject’ especially if enquiring on someone else’s behalf, ‘Third Party’ ensure you have the appropriate documents to confirm their identity, i.e., LPOA, Consent, Court Order.**
2. **If you need to ……**

* Verify whether you are controller of the data subject’s personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller. You may need to assist the controller in complying with any requests they receive.
* Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject. This should be proportionate to the circumstances of the request.
* Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what information is requested? If not: request additional information. Verify whether specific requests are manifestly unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee based on the administrative costs of complying.
* Promptly acknowledge receipt of the SAR and inform the data subject of any permitted costs involved in the processing of the SAR.
* Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.
* Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
* Verify whether the data requested also involves data on other data subjects and make sure this data is excluded before the requested data is supplied to the data subject ;if the third party data cannot be excluded, then it would not be necessary to comply with the request in respect of that requested data unless the other data subject consents to the disclosure or it is reasonable to comply with the request without that other subject's consent.
* Consider whether there are any reasons why certain personal data should not be disclosed where exemptions apply, such as the data is subject to legal privilege or relates to ongoing negotiations with the subject (and where disclosure at that point would prejudice those negotiations).

Responding to a SAR

Make sure to respond to a SAR within one month after receipt of the request:

* If more time is justifiably needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;
* If you are entitled to refuse to comply with the request of the data subject, inform the data subject of this decision without delay and at the latest within one month of receipt of the request.

If a SAR is submitted in electronic form, any information should be provided by electronic means as well.

If data on the data subject is processed, make sure to also include as a minimum the following information in the SAR response:

* The purposes of the processing;
* The categories of personal data concerned;
* The recipients or categories of recipients to whom personal data has been or will be disclosed, including in the case of those in third countries or international organisations, if any appropriate safeguards for transfers of data, such as Binding Corporate Rules or EC-approved model clauses.
* Where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period.
* The existence of the right to request 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.
* If the data has not been collected from the data subject, the source of such data.
* The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Provide a copy of the personal data undergoing processing. This should be provided in a commonly used electronic form if the data subject has submitted the SAR electronically.

If the SAR’s due date falls on a weekend or a public holiday, you have until the next working day to respond. For example, if you receive a request on 25 November, you should respond by 27 December.

# Did you know?

*If you require any help with these requests please do not hesitate to get in touch with your Data Protection Officer Kelly-Anne Gast* [*kelly@almc.co.uk*](mailto:kelly@almc.co.uk) *or 01179 702755*