Information Access (Subject Access Request) Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information Access (Subject Access Request) Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd | Jan 18 New Draft |
| 1.1 | Emma Cooper, Kafico Ltd | Jan 19 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”.Included methods for sending information in digital form  |
| 1.2 | Emma Cooper, Kafico Ltd | Jan 19 – removed reference to charging solicitor for excessive request due to proportionality |
| 1.3 | Emma Cooper, Kafico Ltd | Added section related to Power of Attorney |
| 1.5 | Emma Cooper, Kafico Ltd | Added section for Children and Young People |
| 1.6 | Emma Cooper, Kafico Ltd | Updated Accessing Encrypted Emails Guidance Link |

Contents

[Sources 2](#_Toc17365535)

[1. Scope 2](#_Toc17365536)

[2. Definitions / Context 3](#_Toc17365537)

[3. Clarify the Request 3](#_Toc17365538)

[What Constitutes a Subject Access Request? 3](#_Toc17365539)

[What about Insurance Companies? 4](#_Toc17365540)

[How do I Make Sure a Subject Access Request is Proportionate and Can I charge? 4](#_Toc17365541)

[How Long do I have to Respond? 4](#_Toc17365542)

[How Should I Make Sure I Confirm Identity? 5](#_Toc17365543)

[How Can I Save Time and Costs by Sending Information Digitally? 6](#_Toc17365544)

[What Information Should NOT be Included? 6](#_Toc17365545)

[Children and Young People’s Information 8](#_Toc17365546)

[What about Requests from the Police? 8](#_Toc17365547)

[Appendix A BMI Letter to Patient About Insurance Company Request (language made more accessible to patients) 10](#_Toc17365548)

[Appendix B Letter to Insurance Company Making a SAR 11](#_Toc17365549)

[Appendix D Response to Being Prompted for Timely Response 13](#_Toc17365550)

[Appendix E Using NHS Digital Encryption to send to non nhs.net 14](#_Toc17365551)

[Appendix F Sending SARs by Email 14](#_Toc17365552)

[Appendix G Subject Access Request Refining Response. 14](#_Toc17365553)

[Appendix H Subject Access Request Identification Validation 15](#_Toc17365554)

[Appendix I Subject Access Request Response 16](#_Toc17365555)

[Appendix J Subject Access Request Delay (missed legal deadline) 17](#_Toc17365556)

[Appendix K Request Matrix 18](#_Toc17365557)

## Sources

[Data Protection Act 2018 (DPA)](http://www.legislation.gov.uk/ukpga/2018/12/contents)

[General Data Protection Regulations (EU) 2016/679 (GDPR)](https://gdpr-info.eu/art-9-gdpr/)

[Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)](https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Suffolk.

At the time of writing and unless alternative protocols have been adopted locally, the protocol applies to;

|  |  |  |
| --- | --- | --- |
| Barrack Lane | Martlesham | Mendlesham |
| Burlington Road | Ravenswood | Wickhambrook |
| Framlingham | Stanton (west) | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | The Birches | Framfield |
| Felixstowe Road | Mount Farm | Saxmundham |
| Hawthorn Drive | Swan and Forest | Guildhall & Barrow |
| The Surgery, Leiston | Glemsford | Peninsula |
| Victoria Surgery | Lakenheath | Little St John Street |
| Ivry Street | Ixworth | Grove Medical Centre |

# Definitions / Context

* The GDPR provides the following rights for individuals: The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.
* Individuals have the right to access their personal data.
* The right helps individuals to understand how and why you are using their data, and check you are doing it lawfully.
* This is commonly referred to as subject access.
* Individuals can make a subject access request verbally or in writing.
* You have one month to respond to a request.
* You cannot charge a fee to deal with a request in most circumstances.
* Responsibility for complying with a subject access request lies with the controller and not the processor

# Clarify the Request

There are a number of routes by which information can be sought from practices;

* Subject Access Request
* Access to Medical Reports
* Disclosures to third parties for which there is a legal exemption to data protection principles

## What Constitutes a Subject Access Request?

* A Subject Access Request involves an individual asking for information that is already held about them.
* An individual can ask for information themselves or they can instruct a solicitor or other representative to request the

## What about Insurance Companies?

* When an insurance company makes a Subject Access Request, with the consent of the individual, the template at Appendix A should be sent to the patient and the template at Appendix B should be emailed to the Insurer.
* Practices can charge for requests under the Access to Medical Reports Act because they are producing **new** information and because they are NOT a SAR

## How do I Make Sure a Subject Access Request is Proportionate and Can I charge?

* At this point, we are advised that charging is only for very limited circumstances – repeat copies is main one
* Data subjects are entitled to have all their information without having to explain why they need it
* Sometimes, it might be clear that a solicitor is asking for too much information. For example, they have stipulated that it relates to a back injury sustained in a car accident.
* In this circumstance – they are clearly asking for more information than necessary, so you should call the patient and explain exactly what “full record” means. For example, they may not understand that this includes information about STDs or other stigmatised information
* You should explain that they have a right to limit what is sent to the solicitor
* If they still wish to proceed with full record, you should do so, without any charge
* The practice should always contact the patient to let them know what they are doing in relation to their request
* Postage costs cannot be applied

## How Long do I have to Respond?

* There is a one-month legal time frame for responding to SAR requests
* However, the ICO says;

If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.

You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding to the request begins when you receive the additional information.

* Therefore, when you are communicating with a solicitor for example, in relation to an excessive request, the legal time frame has not yet begun.
* If you are being chased to respond and the requestor has not yet refined the request in a satisfactory way, see **Appendix D** for an appropriate response.

## How Should I Make Sure I Confirm Identity?

* The identity of the person making the request must be validated, using “reasonable means”.
* If you have doubts about the identity of the person making the request you can ask for more information
* However, it is important that you only request information that is **necessary** to confirm who they are. The key to this is proportionality
* This may include information to ensure that a parent has legal guardianship
* You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request.
* The period for responding to the request begins when you receive the additional information

## How Can I Save Time and Costs by Sending Information Digitally?

* If the request is made electronically, the information **should** be provided in a commonly used **electronic** format;
1. Download the clinical records from the system directly into a Word document
2. Provide paper records and Word documents to clinician to highlight information that requires redaction
3. Redact third party information and scan paper records to PDF
4. Send email to patient to confirm they are happy to have information emailed and understand inherent risks with digital transfer, check email address and ask them to confirm receipt
5. Use NHS Digital encryption technique Appendix E
6. Send over several emails where necessary and include the recommended template at Appendix I
* As long as the data subject has put in writing that they understand the inherent risks of using email, the practice can use this route
* If you are required to provide paper copies, you can request collection, but you **cannot** insist
* If a solicitor insists on paper copies (will not accept an email copy) you may charge a fee as can be viewed as excessive
* The text at **Appendix E** should support this.

## What Information Should NOT be Included?

If the requested information contains information about a third party, and releasing it may breach your duty of confidentiality towards that person you should;

* Consider whether it is reasonable to ask their consent
* Consider whether it might be reasonable to release the information without their consent
* Redact the information related to the third party
* Names of professionals are generally not redacted
* Where an individual was present, there is no need to redact information (e.g. Mum and Son attend appointment together, there is no need to redact the other party since they are both already aware).
* It may sometimes be reasonable to release information about a third party – speak to your DPO if you have any concerns

There may be other exemptions to releasing information such as;

* Confidential references
* Publicly available information
* Crime and taxation (where releasing information would prejudice investigation or apprehension or offenders)
* Management information / forecasting
* Negotiations with the requester
* Legal advice and proceedings
* Social work records (where releasing information would prejudice social work activity)
* Health information (where releasing information would cause them harm)
* Information about third parties (not professionals)

Where these additional documents exist, it is important to;

* Acknowledge any confirmation from police / social work departments about whether releasing the information would prejudice their activities.
* Obtain confirmation from clinician about how health information might cause the individual harm
* Whilst you are obtaining these confirmations, if they are taking some time, you could release what you do have.
* Information must not be amended (beyond redaction) for the purposes of releasing under Subject Access Rights.
* When information is released, it is good practice to include;
1. Information about what has been redacted and why
2. A link to <http://www.nhsconfed.org/acronym-buster> which explains abbreviations and terms
3. A link to the practice transparency notice

If you believe that any of these exemptions are applicable, you should contact your DPO for support.

## Children and Young People’s Information

Children and Young People’s information warrants special protection because they are vulnerable.

The age at which children are considered competent to make decisions about their health information is younger than the age they are considered competent to make decisions about their health care (12)

Younger children might also be assessed as competent to make decisions about their information

Unless there are concerns, such as abuse, children’s decisions to keep information from their parents should be respected

If considered to be in best interests of the child (risk of significant harm), disclosure may take place without child’s consent

If a child makes a decision to disclose information and the parents object, parents should usually be informed that the disclosure will take place (unless this would breach duty of confidentiality to the child or young person).

If parents are requesting access to child’s record and the child is competent, access should only be granted with child’s consent

Access should not be granted to information where the child had an expectation of confidentiality (consider sexual health etc) unless in the best interests of the child (Speak with your DPO and consider redaction)

There is a specific exemption regarding child abuse data within a health record when the request comes from someone with parental responsibility. You should speak with your DPO to ensure the exemption is correctly considered as to the best interests of the child.

## What about Requests from the Police?

See **Checklist for Police Disclosures**

It is at the discretion of the practices whether police requests are charged for but there does appear to be a question as to whether such charges would be ethical so our approach is to advise against it.

More templates for responding to SARs are found in the Appendices.

What about Lasting Powers of Attorney?

A lasting power of attorney (LPA) gives a specified person/s (the attorney) legal power to act on another’s behalf (the donor). There are two types of LPA – Health and Welfare & Property and Financial Affairs. Each have a different function and validity.

Health and Welfare LPA

* Only legally effective when the donor is considered to have lost mental capacity
* Cannot override a donor’s wishes on things like DNR that were made in the donors lifetime.

Property and Financial Affairs LPA

* Legally effective from the moment it is signed.
* Gives attorney power to sell the donors property / manage bank accounts and set up care / annuity plans.
* Can have access to basic health data where necessary to decide such details as care home and care / annuity plans.

The donor can set restrictions on the attorney in the LPA documentation so it must always be checked in its entirety when releasing information under an LPA.

In addition, the donor can stipulate whether multiple attorneys can act independently or jointly. Where a donor stipulates they must work jointly, the practice must gain the consent of all attorneys before releasing information to one.

An attorney must act in the best interests of the donor and keep their own affairs separate.

How to respond:

1. Request a copy of the LPA if not provided at the point of request
2. Check LPA to ensure it is the correct document, that it is signed and that there are no restrictions that affect the decision to release information.
3. If it is a Health and Welfare LPA check the mental capacity of the donor. If the patient has not yet lost capacity treat the request as a normal Subject Access Request and liaise with patient themselves to ensure they grant consent.
4. If it is a Financial and Property Affairs LPA ensure the information requested is only for the purposed stated above.
5. Comply with request as per SAR protocol.

# Appendix A BMI Letter to Patient About Insurance Company Request (language made more accessible to patients)

Dear [Patient],

I am writing to you as your insurance company has requested access to your full medical record with your consent – as enclosed.

Because the company has requested your full medical records, we want to check that you understand fully that these records may include extremely sensitive information which you may not expect to be shared or may not need to be shared as part of your application for insurance or the assessment of any claim.

The Information Commissioner’s Office (ICO) has recently written to the insurance industry to advise them to ask for a tailored medical report, rather than the full record because this is seen as requesting more information than is needed to process your claim.

We are therefore giving you a choice. We can provide you with a copy of your **full** medical records under a Subject Access Request so that you can choose whether you give your medical records to the insurance company in full or not.

Alternatively, you can ask your insurer to request a GP report from the practice which will only cover information in your record that is relevant to your application. Medical reports also exclude some information, in line with agreement reached with the insurance industry, such as genetic test results and certain information about sexually transmitted infections.

Please therefore let us know if you would like a copy of your full medical records under a subject access request or whether you plan to ask your insurer to seek a medical report. The BMA has let the Association of British Insurers (ABI) and insurance companies know that we are offering patients this choice. If your insurance company expresses concern about this please ask them to contact the ABI.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

Yours faithfully

# Appendix B Letter to Insurance Company Making a SAR

Dear [Insurer],

I am writing to you in relation to your recent request for the full medical record of {XXX} in relation to an insurance claim.

You are likely aware that the Information Commissioner has been considering the emerging practice of insurance companies obtaining medical records by using patients’ subject access rights.

The ICO recognise that insurance companies may have a genuine need to review medical information about its customers when providing policies like life and critical illness cover.

To enable this, the Access to Medical Reports Act 1988 gives insurance companies a clear and established legal route to access medical information. The Act also gives appropriate safeguards to patients and respects the confidential relationship between a GP and their patient. Under the Act, a GP can provide a tailored report to an insurer, with their patient’s consent, setting out only the information the insurer needs.

However, some insurance companies have instead been looking to rely on the subject access right given to consumers under the Data Protection Act in order to obtain medical records, rather than a tailored GP’s report.

A subject access request gives an individual the right to ask for all of the personal information an organisation holds about them. This is a powerful right, designed to ensure individuals can access information held about them within a specified time period and at a nominal cost. This right was not designed to underpin the commercial processes of insurers.

By making a subject access request on a patient’s behalf, an insurance company may be provided with a patient’s entire medical record, including information that is not relevant for the purpose of underwriting a policy.

The ICO has recently written to the insurance industry to explain that they consider that the use of subject access rights in this way is inappropriate and an abuse of that right.

We have therefore written to the patient to advise them to choose whether they would prefer the entire record to be send directly to them or for a report to be produced by the practice.

Please let us know if you wish to refine your request directly with the practice.

Yours faithfully

# Appendix D Response to Being Prompted for Timely Response

As we have been trying to refine the request and identify exactly what information is required, the time frame for the SAR has not yet begun;

***If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.***

***You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding to the request begins when you receive the additional information.***

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

XXXX surgery are committed to ensuring that they give effect to the rights of data subjects and so, as soon as you have clarified what you need as regards to a proportionate request, or provided payment for a request for full records, the practice will act promptly to provide what you need.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

# Appendix E Using NHS Digital Encryption to send to non nhs.net

1. Send the recipient the guide for accessing encrypted emails for non-NHSmail users
2. Open a new email to the same recipient
3. Type [secure] at the start of the subject line. The word ‘secure’ is not case-sensitive but it must be surrounded by square brackets (no spaces)
4. Ask the recipient to reply to confirm receipt but do not include any patient-identifiable information at this time. This ensures there is no data breach if the recipient email is entered incorrectly.
5. When the recipient replies you can attach the patient-identifiable information, ensuring that [secure] remains at the start of the subject line

[Accessing Encrypted Emails Guidance](https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/Accessing%2BEncrypted%2BEmails%2BGuide.pdf)

# Appendix F Sending SARs by Email

As you will be receiving an email copy of the personal data, that you have requested, we want to point out that whilst we endeavour to use the most secure route possible, we cannot **guarantee** that the message or attachment is virus free or will not been intercepted and amended – these are risks that are inherent to transmitting digital information.

Please reply to confirm that you are understand these risks and are happy to proceed.

# Appendix G Subject Access Request Refining Response.

This response can be used if it is necessary because the individual has not made it clear what information they require.

This should not be used as an approach to delay response.

Dear [insert requestor name],

Thank you for your request for access to information that [insert organisation name] holds about you, which was received by us on [insert date of receipt]. This request will be processed in accordance with Data Protection legislation.

In order for us to ensure that we give you the assistance and support to exercise your information rights, I want to clarify exactly which information you are seeking.

Please could you clarify whether you hope to receive [insert possible option] or [insert possible option].

Once we have this information, we will proceed with processing your request and aim to respond to you within one month.

If we are experiencing a back log, or your request proves to be complex, we may contact you to extend the deadline or to notify you with an explanation of any possible delay.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

We would be happy to discuss this with you further if required.

Sincerely,

[Caldicott Guardian}

# Appendix H Subject Access Request Identification Validation

This response is to ensure that the individual’s identity has been validated. This should be through ‘reasonable’ means.

Dear [insert requestor name],

Thank you for your request for access to information that [insert organisation name] holds about you, which was received by us on [insert date of receipt]. This request will be processed in accordance with the Data Protection Act.

In order for us to ensure that we are not breaching our duty of confidentiality or data protection legislation, we need to verify your identity.

Please I ask that you provide the following;

[insert required evidence or third-party authorisation]

Once we have this information, we will proceed with processing your request and aim to respond to you within one month.

If we are experiencing a back log, or your request proves to be complex, we may contact you to extend the deadline or to notify you with an explanation of any possible delay.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

We would be happy to discuss this with you further if required.

Many Thanks

Sincerely,

[Caldicott Guardian}

# Appendix I Subject Access Request Response

This response should be used for when you are providing a response. You should include an explanation of difficult terms.

If information contained within the record has the potential to cause the individual harm, this should be raised with the DPO.

Dear [insert requestor name],

Thank you for your request for access to information that [insert organisation name] holds about you, which was received by us on [insert date of receipt]. This request will be processed in accordance with the Data Protection Act 2018.

We enclose / attach the requested information.

In line with our duty of confidentiality and data protection legislation we have completed the following;

\* Removed references to third parties where revealing that information would represent a breach of confidence and the individual has not consented

\* Provided this link to a glossary of terms to assist you to understand any coding or complex information <http://www.nhsconfed.org/acronym-buster>

For information about how we use your information and our sharing partners, please visit [insert link to practice transparency notice]

We hope that you have all the information that you require.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

We would be happy to discuss this with you further if required.

Many Thanks

Sincerely,

[Caldicott Guardian}

# Appendix J Subject Access Request Delay (missed legal deadline)

This response can be used where the legal deadline has been missed. This is now an information breach and so it should be recorded as such and discussed with the DPO.

Dear [insert requestor name],

Thank you for your request for access to information that [insert practice name] holds about you, which was received by us on [insert date of receipt].

At present we have [insert number of requests] awaiting resolution and it is taking some time to work through these and provide the information required.

We anticipate that we will be able to respond by [insert date]

We sincerely apologise for any issues or frustration this may cause you and assure you that we are working hard to provide you the information you have requested. If you only require a part of your record, please let us know as it will help us to respond sooner.

You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Additionally, you also have a right to seek to enforce your rights through the courts.

We would be happy to discuss this with you further if required.

Many Thanks

Sincerely,

[Caldicott Guardian}

# Appendix K Request Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   |   |   |   |   |
| **DESCRIPTION** | **Subject Access Request** | **Non-healthcare activity - chargeable** | **Access to Medical Records Act** | **Other** |
| Shotgun Licence  |   |   |   |   |
| Driving Licence  |   |   |   |   |
| Passport - verify identity  |   |   |   |   |
| Fitness to: letter, certificate, attend gym |   |   |   |   |
| Holiday Cancellation Certificate - Complex |   |   |  |  |
| Holiday Cancellation Certificate - Medium |   |   |  |  |
| Holiday Cancellation Certificate - Simple |   |   |  |  |
| Copy of Sick Note |   |   |   |   |
| Letter request  |   |   |   |   |
| Sick Note for School (private paper certificate - no charge) letter |   |   |   |   |
| To Whom It May Concern letter: Simple One Liner |   |   |   |   |
| To Whom It May Concern letter: Medium |   |   |   |   |
| To Whom It May Concern letter: Lengthy |   |   |   |   |
| Private Treatment Verification |   |   |   |   |
| Medication List for patients travelling |   |   |   |   |
| Letter from GP to go with medication list for travelling  |   |   |   |   |
| Reports for employers |   |   |   |   |
| Reports for Housing |   |   |   |   |
| Request from solicitor acting on behalf of patient |   |   |   |   |
| Request from solicitor NOT acting on behalf of patient |   |   |   |   |
| Claims company acting on behalf of patient |   |   |   |   |
| Insurance company with consent from patient but acting for their own commercial purposes i.e. the patient is trying to claim and insurance company validating the claim |   |   |   |   |
| Police asking for records in relation to a crime |   |   |   |   |
| Army requesting medical records |   |   |   |   |
| Court orders records to be disclosed |   |   |   |   |
| Patient / their rep requests copy of all or some of their records |   |   |   |   |