INFORMATION GOVERNANCE:

SUBJECT ACCESS REQUEST POLICY

Policy Header	
Applies to	All staff and stakeholders
Date issued	2023-12-15
Status	Ratified
Version	5.0
Date for review	2025-12-15

DOCUMENT CONTROL

Version	Date	Summary of Changes
1.0	2018-03-01	Initial version
2.0	2019-03-19	Reviewed
3.0	2020-03-20	Reviewed
4.0	2021-04-09	Reviewed – updated
5.0	2021-12-23	Updated and included flowchart – revised policy
6.0	2023-12-15	Reviewed and updated (DPA version updated)

DEFINITIONS

Term	Definition
Organisation	Medical Clinics Ltd
DPA	The Data Protection Act 2018 https://www.gov.uk/data-protection
GDPR	General Data Protection Regulation https://gdpr-info.eu/
SAR	Subject Access Request

ICO	Information Commissioner's Office https://ico.org.uk/
FOI(A)	Freedom of Information / Freedom of Information Act https://www.gov.uk/make-a-freedom-of-information-request
EIR	Environmental Information Regulation http://www.legislation.gov.uk/uksi/2004/3391/contents/made

CONTENTS

Contents

POLICY

1 INTRODUCTION

1.1: Individuals have rights under the DPA and GDPR, subject to certain exemptions, to access to their personal records that are held by the Organisation. This is known as a 'subject access request' (SAR). Requests may be received from members of staff, service users or any other individual who the Organisation has had dealings with and holds data on. This will include information held both electronically and manually and will

therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

1.2: The Organisation has developed this policy to guide staff in dealing with SARs that may be received. The aim of this policy is to inform employees on how to advise service users on how to make a SAR, how to recognise a SAR and know what action to take on receipt. This procedure sets out the processes to be followed to respond to a SAR. This is based on the ICO's Subject Access Code of Practice: ICO Subject Access Code of Practice.

1.3: This policy has been developed based on the knowledge and experience of the Information Governance Team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

2 WHAT IS A SUBJECT ACCESS REQUEST?

2.1: A SAR is simply a written or verbal request made by or on behalf of an individual for the information about them, which is held by the Organisation. The Data Protection Legislation entitles all individuals to make requests for their own personal data to enable individuals to verify the lawfulness of how their information is being processed.

2.2: An individual is not entitled to information relating to other people (unless they are acting on behalf of that person). The request does not have to be in any particular form, nor does it have to include the words 'subject access' or make any reference to the Data Protection Legislation or GDPR.

2.3: A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore be treated as a SAR in the normal way.

2.4: The applicant must be informed of how the application is being dealt with and under which legislation.

2.5: The application must be free of charge, except where the request is manifestly unfounded or excessive.

2.6: Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

i. Told whether any personal data is being processed;

ii. Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisation or people;

iii. Given a copy of the data in question;

iv. Given details of the source of the data (where this is available);

2.7: Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also other restrictions on disclosing information in response to a SAR, for example where this would involve disclosing information about another individual.

3 HOW TO RECOGNISE AND ACTION A SUBJECT ACCESS REQUEST

3.1: In order for the Organisation to action a SAR the following must be received:

i. The request must be made in writing (This may be by letter, fax, email, or even social media, such as Facebook or Twitter) or verbally. It is important to note that responses to SAR requests must be returned by a secure methodology, i.e., social media must NOT be used to return information requested;

ii. Any fee levied, fees can only be levied where the request is deemed manifestly unfounded or excessive;

iii. Proof of identity of the applicant and/or the applicant representative, and proof of right of access to another person's personal information, by reasonable means;

iv. Sufficient information to be able to locate the record or information requested;

v. All requests must be responded to without delay and at the latest within one month of receipt of the request. This time can be extended by a further 2 months where requests are complex or numerous. However, if this is the case you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

3.2: If the request relates to, or includes information that should not be requested by means of a SAR (e.g., it includes a request for non-personal information) then the request must be treated accordingly, e.g., as a FOI request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under the DPA and GDPR; and another for the remaining, non-personal information made under FOIA.

3.3: If any of the non-personal information is environmental, this should be considered as a request made under the Environmental Information Regulations (2004). Any requests made for non-personal information must be forwarded to the FOI Team.

3.4: It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOIA or the EIR is to the world at large – not just the requester. If personal data is mistakenly

disclosed under FOIA or the EIR to the world at large, this could lead to a breach of the data protection principles.

3.5: All SAR requests received must be forwarded to the relevant head of department, e.g. employees requesting access to personnel records must be sent to Head of HR, without delay, for it to be processed within the legal timescale.

3.6: Where the Organisation processes a large quantity of information about an individual the GDPR permits you to ask the individual to specify the information the request relates to. The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

3.7: Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

i. Charge a reasonable fee taking into account the administrative costs of providing the information;

ii. Refuse to respond (where you refuse to respond you must explain 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).

4 ASSISTING AND ADVISING SERVICE USERS ON HOW TO MAKE A REQUEST

4.1: Where an individual is making a request, you should advise them that they will need to:

i. Put the request in writing where possible, detailing the information they are requesting and from which service to enable it to be located;

ii. Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request;

iii. A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So, it is important to ensure that you and your colleagues can recognise a SAR and deal with it in accordance with this procedure and forward immediately to the relevant service head;

iv. Advise the applicant to send the request to the appropriate head of service, and provide contact details;

v. Where an applicant is unable to put the request in writing assistance should be given to them to make the request verbally, best practice would be to document the request details in an

accessible format for the applicant and request them to confirm the details are correct. Applicants can be referred to the Administration Team to obtain appropriate assistance in making their application.

vi. Note that responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed e.g., braille or additional languages,

5 REQUESTS MADE ABOUT OR ON BEHALF OF OTHER INDIVIDUALS

5.1: **General Third Party**: A third party, e.g., solicitor, may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g., power of attorney must be provided by the third party. If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

5.2: Requests on Behalf of Children: The UK GDPR does not give a specific age for data consent for children; however, it does state that children aged 13 an over can consent to their data being shared with information society services. Therefore, it is reasonable to assume that any child aged 13 or above must consent before their information can be shared with a third party, even if that third party has parental responsibility. If a child is under the age of 13 a third party with parental responsibility may make a SAR on behalf of the child even without the explicit consent of the child.

5.3: Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child has the capacity to understand their rights and any implications of the disclosure of information, then child's permission should be sought to action the request where appropriate given point 5.2.

5.4: The GDPR indicates that in most cases it would be reasonable to assume that any child that is aged 13 years or more would have the capacity to make a SAR and should therefore be consulted in respect of requests made on their behalf.

5.5: The Caldicott Guardian or their nominated representative should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that, just because a child has capacity to make a SAR, that they also have capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so. What matters is that the child can understand

(in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following should be considered:

i. Where possible, the child's level of maturity and their ability to make decisions like this;

ii. The nature of the personal data;

iii. Any court orders relating to parental access or responsibility that may apply;

iv. Any duty of confidence owed to the child or young person;

v. 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;

vi. Any detriment to the child or young person if individuals with parental responsibility cannot access this information;

vii. Any views the child or young person has on whether their parents should have access to information about them.

6 REQUESTS IN RESPECT OF CRIME

6.1: Requests for personal information may be made by authorities such as the Police or the HMRC for the following purposes:

i. The prevention or detection of crime;

ii. The capture or prosecution of offenders;

iii. The assessment or collection of tax or duty.

6.2: A formal documented request signed by a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

6.3: These types of requests must be considered by a senior manager and the decision on whether to share the information or not documented before any action is taken. Advice can be sought from the Information Governance Team.

6.4: **Court Order**: Any court order requiring the supply of personal information about an individual must be complied with.

7 RESPONDING TO REQUESTS

7.1: It is essential that a log of all requests received is maintained, detailing:

i. Date received;

ii. Date Response due (within one calendar month unless complex);

iii. Applicant's details;

iv. Information requested;

v. Exemptions applied in respect of information not to be disclosed;

vi. Details of decisions to disclose information without the subject's consent;

vii. Details of information to be disclosed and the format in which they were supplied;

viii. When how the information was supplied, e.g., *paper copy* by *post*.

7.2: Determine whether the person's request is to be treated as a routine enquiry or as a SAR. If you would usually deal with the request in the normal course of business, e.g., confirming appointment times or details of public meetings planned then do so. The following are likely to be treated as formal subject access requests:

i. "Please send me a copy of my HR file or Medical Records";

ii. "I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed";

iii. "The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer".

7.3: Ensure adequate proof of the identity of both the data subject, and the applicant where this is a third party, is obtained before releasing information requested.

7.4: Ensure adequate information has been received to facilitate locating the information requested. Locate the required information from all sources and collate it ready for review by an appropriate senior manager. This review is to ensure that the information is appropriate for disclosure, i.e., to ascertain whether any exemptions apply e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed or is information to be withheld due to on-going formal investigations.

7.5: Advice may be sought from the Information Governance Team. Exemptions are detailed at Appendix B. In the case of requests for clinical records these should be reviewed by the Caldicott Guardian or a nominated representative who shall decide to what extent data can be disclosed or whether the request is to be refused.

7.6: Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual. However, information contained within the information requested was supplied by health professionals it may be disclosed without consent if considered appropriate.

7.7: Generally, the Organisation must provide a copy of the information free of charge. However, a 'reasonable fee' may be levied when a request is manifestly unfounded or excess, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

7.8: Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact as soon as possible.

7.9: It must be determined whether the information is likely to change between receiving the request and sending the response. Routine on-going business additions and amendments may be made to the personal information after a request is received, however the information must not be altered because of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under the DPA.

7.10: Check whether the information collated contains any information about any other individuals and if so, consider:

i. Is it possible to comply with the request without revealing information that relates to the third party;

ii. Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party;

iii. Has the third party consented to the disclosure;

iv. Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party;

v. Duty of confidence owed to the third party;

vi. Steps taken to try and obtain consent;

vii. Whether the third party can give consent;

viii. Any express refusals of consent from the third party;

ix. A record of the decision as to what third party information is to be disclosed and why should be made.

7.11: Consider whether you are obliged to supply the information, i.e., consider whether any exemptions apply in respect of:

i. Crime prevention and detection, including taxation purposes;

ii. Negotiations with the requestor;

iii. Management forecasts;

iv. Confidential references given by you;

v. Information used in research, historical or statistical purposes;

vi. Information covered by legal professional privilege;

vii. Other exemptions are detailed at **Appendix B**;

7.12: If the information requested is held by the Organisation and exemptions apply, then a decision must made as to whether you inform that applicant that the information is held but is exempt from disclosure or whether you reply stating that no relevant information is held.

7.13: A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing on-going or potential investigations or undue harm or distress is to be avoided. NB: It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered.

7.14: If the information contains complex terms or codes, you must ensure that these terms and codes are explained in such a way that the information can be understood in lay terms. Preparing the response:

i. When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case, by the due date;

ii. A copy of the information should be supplied in a format agreed with the applicant for example if the request is received electronically, then the response should be returned in an electronic format.

iii. You have one calendar month to comply with the request starting from the date you receive all the information necessary to deal with the request and any fee that is required.

iv. It is an offence under the Data Protection Legislation and individuals can complain to the ICO or apply to a court if you do not respond within this time limit;

v. NB: Under no circumstances should original records be sent to the applicant.

8 IMPLEMENTATION

8.1: This policy will be published on the Organisation's intranet and all staff will be made aware of its publication through communications and team meetings.

8.2: Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence.

8.3: The Senior Management Team and line managers are responsible for ensuring that all staff are aware of the policy which will be available on the Organisation intranet.

8.4: Performance against the Data & Security Protection Toolkit will be reviewed on an annual basis and used to inform the development of future procedural documents. This standard will be reviewed on a regular basis, and in accordance with the following on an as and when required basis:

i. Legislative changes;

ii. Good practice guidance;

iii. Case law;

iv. Significant incidents reported;

v. New vulnerabilities;

vi. Changes to organisational infrastructure.

8.5: This policy and procedure will be reviewed at least every three years by the Organisation in conjunction with managers, with changes made as required and the outcome published. Where a review is necessary due to legislative change, this will happen immediately.

9 DATA SUBJECT RIGHTS REQUESTS

9.1: Data subjects may also make other types of requests to the data controller regarding the information held by the organisation.

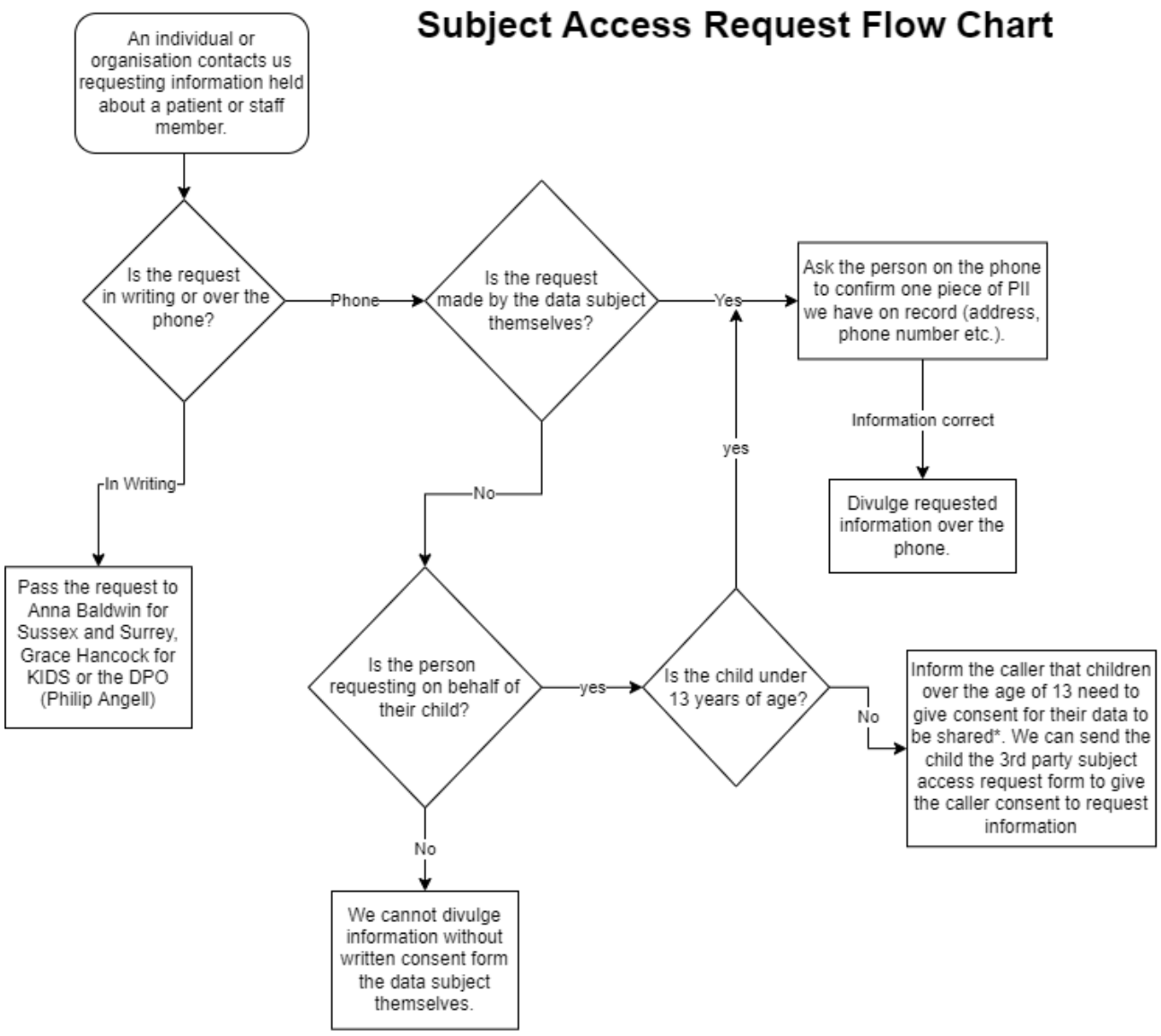
9.2: These rights include; the right to erasure, the right to rectification and the right to limit processing. (full list on privacy notice).

9.3: Where possible these requests will be handled using the same controls laid out above for SARs, including the methods for authenticating data subjects and obtaining consent.

9.4: As with SARs these requests are subject to the relevant data protection regulations and exemptions.

10 APPENDIX A: Flow Chart

10.1: Flow chart for individuals to respond to SARs:



* If the data that is requested is confirmation of prerequisites for the appointment or time and location of already booked appointments the information can be shared with parents of children over the age of 13. There are some situations where this can be delicate, for example split families, if you are unsure of the correct course of action refer the request to Anna Baldwin for Sussex and Surrey, Grace Hancock for KIDS or the DPO (Philip Angell)

11 APPENDIX B: SUBJECT ACCESS REQUEST EXCEPTIONS

11.1: **National security:** Personal information that is held in respect of the maintenance of national security is exempt from disclosure.

11.2: **Crime and taxation:** Section of the personal information contained in the records, or individual records that relate to the prevention and detection of crime or the apprehension or prosecution of offenders.

11.3: **Health, education and social work:** Health exemptions are mentioned in section 7 Social work records exemptions comes under the Data Protection (Subject Access Modification) (Social Work) Order 2000 relates to personal

information used for social work purposes: Where release of information may prejudice the carrying out of social work by causing serious harm to the physical or mental condition of the data subject or others. Certain third party's information can be released if they are a "relevant person" (a list is contained in the order) as long as release of the information does not cause serious harm to the relevant person's physical or mental condition, or with the consent of the third party.

11.4: **Regulatory activity:** Personal data processed for the purposes of discharging functions are exempt if the release of such information would prejudice the proper discharge of those functions. Research, history statistics Where the personal data is used solely for research purposes and if resulting statistics are not made available which identify the person.

11.5: **Human fertilisation and embryology:** Personal information can be withheld in certain circumstances where it relates to human fertilization and embryology.

11.6: **Legal professional privilege**: Any correspondence to or from or documentation prepared for or by the Organisation's internal or external legal advisors may be exempt from disclosure and advice should always be sought relating this class of information.

END OF DOCUMENT