Information Governance

SAR Policy & Procedure

Policy Reference: OHCPWHN/IG/SARP V1

Policy Title	SAR Policy	
Author/Contact	Holly Hellstrom – Information Assurance Director	
Document Ref	OHCPWHN/IG/SAR	
Version	1	
Status	Approved	
Publication Date	April 2023	
Review Date	May 2026	
Approved by	Dr James Britton – Caldicott Mr Jeremy Fowler – SIRO	17th April 2023
Ratified by	IG Team	17th April 2023

Version	Date	Comments	Author
1	17/4/2023	IGT	Information Assurance Director

Contents

BACKGROUND

Ozone Health Ltd is the overarching board and governance for Ozone Health Ltd (OHL), Clinical Partnership (CP) & The World Healthnet Ltd (WHN).

INTRODUCTION

Individuals have the right under current Data Protection legislation and the General Data Protection Regulation (UK) subject to certain exemptions, to have access their personal records that are held by the group or one of our organisations. 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 company has had dealings with and holds data about that individual. 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, and audio recordings etc.

PURPOSE

The Group has developed this policy to guide staff in dealing with Subject Access Requests that may be received in line with the Legislation to promote transparency and openness and supports all individuals (service users and employees) when exercising their right to access.

The aim of this policy is to inform staff on, how to advise service users on how to make a subject access request, how to recognise a subject access request and know what action to take on receipt.

This procedure sets out the processes to be followed to respond to a subject access request**.** This is based on the Information Commissioner's Office Subject Access Code of Practice: ICO Subject Access Guidance

DEFINITIONS

Term	Definition
Data Protection Act 2018	The Data Protection Act updates our data protection laws for the digital age. It received Royal Assent in May 2018 and replacesthe Data Protection Act 1998
Access to Health Records 1990	**Access to Health Records** Act **1990** act to establish a right of **access** to **health records** by the individuals to whom they relate and other persons; to provide for the correction of inaccurate **health records** and for the avoidance of certain contractual obligations; and for connected purposes
Personnel Records	Personnel records can be records in a **computerised** or in a **manual** form or a mixture of both. These can be held by our Human Resources.

ENGAGEMENT

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 healthcare organisations.

SCOPE

The policy applies to the Group and all its employees and must be followed by all those who work for the organisation, including contractors, those on temporary or honourary contracts, secondments, pool staff and students.

The Group has a legal obligation under current Data Protection Legislation to ensure compliance with individual's right of access to personal information held by the Group or one of their companies, therefore breach of this policy will be regarded as serious misconduct and may result in:

- dismissal.
- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures.
- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and
- legal action being taken against the discloser and/or any other third party.

DUTIES & RESPONSIBILITIES

Overall accountability for procedural documents across the organisation lies with the Accountable Officer, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

The Group Caldicott Guardian and SIRO, and IG Team/DPO are responsible for overseeing and advising on disclosure of individual's information held by the Group or one of their companies.

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors, and volunteers, know what is expected of them should they receive a subject access request from a service user or other member of the public. In addition, they should be aware of what information they should supply to the officer responsible for the management of Subject Access Requests within the Group.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR)/Data Protection Act 2018 includes the requirement to complete a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals.

The Group is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and

confidentiality guidance. More detailed information can be found in the Data Protection & Confidentiality Policy and related policies and procedures.

POLICY PROCEDURAL REQUIREMENTS

How to recognise a Subject Access Request

In order for the Group to action a subject access request the following must be provided by the applicant and then the following steps should be followed:

- The request for information, this does not need to be in any particular format and does not need to mention it is subject access request or the Data Protection Act. It may be made in writing (This may be by letter, email, or even social media, such as Facebook or Twitter). The request may be made verbally, where this occurs a record of the request must be made detailing the information requested, the date requested and by whom.

- Proof of identity of the applicant and/or the applicant's representative, and proof of right of access to the data subject's personal information, by reasonable means (See Appendix A) must be obtained.

- The request must contain sufficient information to be able to locate the record or information requested.

- All requests must be responded to without delay and at the latest within one month of receipt of the request, the one calendar month starts on the receipt of appropriate proof of identity. 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.

- 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 Freedom of Information (FOI) request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under Data Protection Legislation; and another for the remaining, non- personal information made under FOI Legislation. If any of the non-personal information is environmental, this should be considered as a request made under the Environmental Information Regulations (EIR).

Any requests made for non-personal information must be forwarded to the FOI Team at governance@ozonehealth.co.uk. It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOI Legislation or the EIR is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOI Legislation or the EIR to the world at large, this could lead to a breach of the data protection principles.

All SAR requests received must be forwarded to Officer responsible for the management of SARs.

Data Protection Legislation 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. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

a) Charge a reasonable fee taking into account the administrative costs of providing the information; or
b) Refuse to respond.

Where you refuse to respond you must explain the reason for the refusal 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.

Responses to SAR requests must be returned by a secure methodology, such as the NHS Mail Secure service i.e., social media must **NOT** be used to return information requested.

Assisting and advising services users in making a request

Where an individual is verbally making a request, you should:

- Make a written record of the request, detailing the information being requested and from which service to enable its location and verify with the requestor that the written record is correct.

- 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. Note some requestors may require additional assistance and therefore details might have to be supplied in an alternative accessible format, e.g., braille.

- 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 appropriately, and ensure it is forwarded immediately to the officer within the Group responsible for dealing with the SAR's at governance@ozonehealth.co.uk.

- Obtain the requestors contact details, proof of identity and details on how they would like the response to the application to be returned to them. Note that responses to requests should be made in a format requested by the requestor, therefore alternative formats may be needed e.g., braille.

General Third Party

- A third party, e.g., solicitor or relative 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 individual's 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 who is the subject of the SAR rather than to the third party and inform the third party that the information has been sent directly to the data subject. The individual may then choose to share the information with the third party after having had a chance to review it.

Requests on Behalf of Children

- Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

- 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 the child's permission should be sought to action the request.

- The Information Commissioner has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

- 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 is able to 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 taken into account:
    - Where possible, the child's level of maturity and their ability to make decisions like this.
    - The nature of the personal data.
    - Any court orders relating to parental access or responsibility that may apply.
    - Any duty of confidence owed to the child or young person.
    - 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.
    - Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
    - Any views the child or young person has on whether their parents should have access to information about them.

Requests in respect of Crime and Taxation e.g., from the Police or HMRC

- Requests for personal information may be made by the above authorities for the following purposes:
    - The prevention or detection of crime.
    - The capture or prosecution of offenders; and
    - The assessment or collection of tax or duty.

- 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.

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

Court Orders

- Any Court Order requiring the supply of personal information about an individual must be complied with. If the order is unclear, for example whether the court requires the information in a redacted or unredacted form, it is reasonable to check this with the court prior to disclosure.

RESPONDING TO REQUESTS

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

- Date received,
- Date response due (within one calendar month unless complex),
- Applicant's details,
- Information requested,
- Date the response was sent,
- Exemptions applied in respect of information not to be disclosed,
- Details of decisions to disclose third party personal data without the data subject's consent,
- Details of information to be disclosed and the format in which they were supplied,
- When and how supplied, e.g., Paper copy and postal method used to send them.

- Determine whether the person's request is to be treated as a routine enquiry or as a subject access request. 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.
  - Please send me a copy of my HR file or Medical Records.
  - I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed.
  - The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.

- Ensure adequate proof of the identity of both the data subject and the applicant, where this is a third party is obtained before releasing any information requested, this may be in the form of documentation as detailed at Appendix A.

- 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. 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.

Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual, unless it is information that would clearly already be known by the applicant, e.g., the names of other members of their family. Where information contained within the information requested was supplied by health professionals it may be disclosed without consent if considered appropriate.

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

- 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.

- 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 as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under Data Protection Legislation.

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

- Is it possible to comply with the request without revealing information that relates to the third party?
  (Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party)

- Where it is not possible to remove third party identifiers you must consider the following.
  - Has the third party consented to the disclosure?
  - Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party?

(The following must be considered when trying to determine what reasonable circumstances are);

- duty of confidence owed to the third party,
- steps taken to try and obtain consent,
- whether the third party is capable of giving consent, and
- any previous express refusals of consent from the third party.

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

- Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:
  - Crime prevention and detection, including taxation purposes,
  - Negotiations with the requestor,
  - Management Forecasts,
  - Confidential References given by you,
  - Information used in research, historical or statistical purposes; and
  - Information covered by legal professional privilege.

Other exemptions are detailed at Appendix B.

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. 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.

- 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:

  - When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case, by the due date.
  - 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. You have one month to comply with the request starting from the date you receive all the information necessary to deal with the request. It is an offence under the Data Protection Legislation and individuals can complain to the Information Commissioner's Office or apply to a court if you do not respond within this time limit.
  - **NB** Under no circumstances should original records be sent to the applicant.

- Remote access to records: - Where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

- The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

- Ensure that the information to be supplied is reviewed by an appropriate senior manager and written authorisation and / or agreement of exemptions applied is obtained for disclosure or non-disclosure of the information.

REFUSING A REQUEST

- If an exemption applies, you can refuse to comply with a subject access request (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information see the ICO website.

- You can also refuse to comply with a subject access request if it is:
  - manifestly unfounded; or
  - excessive.

- Where it is decided to refuse a request, you must be very sure of your legal basis for doing this and you should ask your Data Protection Officer for advice. You should also inform your SIRO as they will need to make the final decision.

- You must inform the individual without undue delay and within one month of receipt of the request.

- You should inform the individual about:
  - the reasons for the decision.
  - their right to make a complaint to the ICO or another supervisory authority; and
  - their ability to seek to enforce this right through a judicial remedy.

- You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

- You must ensure that you fully document the decision and the reasoning behind it in case of further challenges.

IMPLEMENTATION

This policy will be published on our website(s) and all staff will be made aware of its publication through communications and team meetings.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the company procedures.

TRAINING AND AWARENESS

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 SharePoint.

MONITORING AND AUDIT

Performance against the DSPToolkit 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:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

COMPLAINTS

If an individual or their representative is not satisfied with the outcome of their request, for example, if they feel information has been withheld or recorded incorrectly, or that they have not been allowed sufficient time to view the information, they should be informed of the options available to them to take further action.

In the first instance, the individual should be encouraged to attend an informal meeting with a view to addressing and resolving the issues locally with the Information Assurance Team.

An individual also has the option to escalate the matter to the Caldicott Guardian for review.

An individual can escalate the matter to the ICO using the following contact details:

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Tel: 01625 545745
E-mail: mail@ico.gsi.gov.uk

POLICY REVIEW

The policy and procedure will be reviewed at least every three years by the company in conjunction with managers, and Trade Union representatives if appropriate, with changes made as required and the outcome published. Where review is necessary due to legislative change, this will happen immediately.

Audit and Governance Teams has delegated responsibility for monitoring and reviewing the policy and will report any concerns to the Governing Body.

REFERENCE DOCUMENTS

- Data Protection Act 2018
- General Data Protection Regulation (UK)

CROSS REFERENCE

- Confidentiality & Data Protection Policy
- National Opt Out Policy
- Record Management and Lifecycle Policy

APPENDIX A - REGISTRATION & AUTHENTICATION EXAMPLES OF DOCUMENTARY EVIDENCE

Please supply one from each of the following categories (copies only).

- current signed passport
- residence permit issued by Home Office to EU Nationals on sight of own country passport
- current UK photocard driving licence
- current full UK driving licence (old version) – old style provisional driving licences are not acceptable
- current benefit book or card or original notification letter from the Department for Work & Pensions confirming the right to benefit
- building industry sub-contractor's certificate issued by the Inland Revenue
- recent Inland Revenue tax notification
- current firearms certificate
- birth certificate
- adoption certificate
- marriage certificate
- divorce or annulment papers
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms);
- GV3 form issued to people who want to travel in the UK but do not have a valid travel document
- Home Office letter IS KOS EX or KOS EX2
- police registration document
- HM Forces Identity Card

Active in the Community

"Active in the Community" documents should be recent (at least one should be within the last six months unless there is a good reason why not) and should contain the name and address of the registrant.

- record of home visit
- confirmation from an Electoral Register search that a person of that name lives at that address
- recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed)
- local authority Council Tax bill (valid for current year)
- current UK photo card driving licence (if not used for evidence of name)
- current full UK driving licence (old version) (if not used for evidence of name)
- bank, building society or credit union statement or passbook containing current address
- recent original mortgage statement from a recognised lender
- current local council rent card or tenancy agreement
- current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit
- court order

APPENDIX B – SUBJECT ACCESS REQUESTS EXEMPTIONS

This is not an exhaustive list, for comprehensive information on how to apply exemptions see the code of practice.

Category	**Exemption**
National Security	Personal information that is held in respect of the maintenance of national security is exempt from disclosure.
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
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
Regulatory activity	Personal data processed by the group for the purposes of discharging it 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 as long as resulting statistics are not made available which identify the person.
Human fertilisation and embryology	Personal information can be withheld in certain circumstances where it relates to human fertilisation and embryology.
Legal Professional Privilege	Any correspondence to or from or documentation prepared for or by internal or external legal advisors may be exempt from disclosure and advice should always be sought relating this class of information.