NHS
Staffordshire and
Stoke-on-Trent
Integrated Care Board

Guidance and Standard Operating Procedure for the Management of Subject Access Requests

.

Information Reader Box	
Directorate	Corporate
Purpose	Guidance
Document Purpose	Procedures
Version	3.0
Document Name	Standard Operating Procedure for the Management of Subject Access Requests
Author	Governance Manager/IG Operational Lead
Publication Date	01 July 2025
Review Date	01 July 2026 or as national/legislation changes dictate
Target Audience	All staff employed by: Staffordshire and Stoke-on-Trent Integrated Care Board (ICB)
Description	Standard Operating Procedure for the Management of Subject Access Requests
Superseded Document	N/A
Action Required	To Note
Contact Details and further information	ICB Governance Team

Document Status
This is a controlled document. Whilst this document may be printed, the electronic version posted on the internet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet

Contents

1.0 INTRODUCTION

This procedure applies to The Integrated Care Board ('the ICB') and all its Subject Access Requests (SAR) duties.

The right of access, commonly referred to as Subject Access Request (SAR), gives individuals the right to obtain a copy of their personal data from the organisation, as well as other supplementary information. It helps individuals understand how and why the organisation uses their data and check it is being done lawfully.

An individual can make a request verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

An individual may ask a third party (i.e. a relative, friend or solicitor) to make a SAR on their behalf. A SAR may also be made on behalf of an individual through an online portal, before responding, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

An individual may only request information relating to themselves. They cannot request information relating to a third party, the third party should submit their own request.

This document is based on the Information Commissioner's Office Subject Access Code of Practice and sets out the process for handling Subject Access requests received in the ICB's offices. It is intended to assist those members of staff who are involved in providing responses / investigations into Subject Access requests, including employees of the ICB and providing guidelines for timescales in which Subject Access requests should be responded to.

2.0 Our Obligations under the UK GDPR Act

The ICB's obligation under the current Data Protection legislation and the UK General Data Protection Regulation (GDPR) Right of Access Act is to respond to valid requests for information that the ICB hold about them. In most cases the ICB has one calendar month in which to respond to a SAR.

Important Notes in relation to response timeframes:

2.1 The one calendar month starts on the receipt of appropriate proof of the requester's identity.

2.2 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.

2.3 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.

2.4 You can't add extra days when the calendar month is shorter. For example, if you receive a request on the 31 January, you should respond by the 28 February.

2.5 You may extend the time to respond by a further two months if requests are complex or numerous.

3.0 What is personal data

Personal data is information that relates to an identified or identifiable individual. Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

The UK GDPR applies to the processing of personal data that is:

3.1 Information that relates to an identified or identifiable individual

3.2 Data that can directly identify an individual from the information held.

3.3 Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

3.3 Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

3.4 If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.

3.5 Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

3.6 Information about companies or public authorities is not personal data.

3.7 However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

For clarity anything that can potentially be ruled "exempt" will be as per the ICO guidance and will be handled on a case-by-case basis by the Governance team and yourselves and in line with the guidance Right of access/subject access requests and other rights \| ICO

4.0 What are Identifiers and related factors?

An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.

4.1 A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context.

4.2 A combination of identifiers may be needed to identify an individual.

4.3 The UK GDPR provides a non-exhaustive list of identifiers, including:

4.4 name;

4.5 identification number;

4.6 location data; and

4.7 an online identifier.

4.8 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.

4.9 Other factors can identify an individual.

Can we identify an individual directly from the information we have?

4.10 If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).

4.11 You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.

4.12 If an individual is directly identifiable from the information, this may constitute personal data.

Can we identify an individual indirectly from the information we have (together with other available information)?

4.13 It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.

4.14 Even if you may need additional information to be able to identify someone, they may still be identifiable.

4.15 That additional information may be information you already hold, or it may be information that you need to obtain from another source.

4.16 In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.

4.17 When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.

4.18 You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

What is the meaning of 'relates to'?

4.19 Information must 'relate to' the identifiable individual to be personal data.

4.20 This means that it does more than simply identifying them – it must concern the individual in some way.

4.21 To decide whether or not data relates to an individual, you may need to consider:
- 4.21.1 the content of the data – is it directly about the individual or their activities?;
- 4.21.2 the purpose you will process the data for; and
- 4.21.3 the results of or effects on the individual from processing the data.

4.22 Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them. In this case any information that is not relative to the individual should be redacted.

4.23 There will be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.

4.24 Inaccurate information may still be personal data if it relates to an identifiable individual.

What happens when different organisation's process the same data for different purposes?

4.25 It is possible that although data does not relate to an identifiable individual for one controller, in the hands of another controller it does.

4.26 This is particularly the case where, for the purposes of one controller, the identity of the individuals is irrelevant, and the data therefore does not relate to them.

4.27 However, when used for a different purpose, or in conjunction with additional information available to another controller, the data does relate to the identifiable individual.

4.28 It is therefore necessary to consider carefully the purpose for which the controller is using the data in order to decide whether it relates to an individual.

4.29 You should take care when you make an analysis of this nature.

For clarity anything that can potentially be ruled "exempt" will be as per the ICO guidance and will be handled on a case-by-case basis by the Governance team and yourselves and in line with the guidance Right of access/subject access requests and other rights \| ICO

5.0 Can the right of access be enforced?

Yes. In appropriate cases, the ICO may take action against a controller if they fail to comply with data protection legislation. The ICO may exercise its enforcement powers in accordance with their Regulatory Action Policy.

6.0 What is the right to rectification?

If a SAR reveals that a person's data is inaccurate or incomplete, they have the right to have the information rectified according to Article 16 of the UK GDPR.

What do we need to do?

6.1 If you receive a request for rectification, you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject, if in doubt contact the ICB Governance team.

7.0 Exemptions

7.1 The UK GDPR and the Data Protection Act 2018 set out exemptions from some of the rights and obligations in some circumstances.

7.2 Whether or not you can rely on an exemption often depends on why you process personal data.

7.3 You should not routinely rely on exemptions; you should consider them on a case-by-case basis.

7.4 You should justify and document your reasons for relying on an exemption.

7.5 If no exemption covers what you do with personal data, you need to comply with the UK GDPR as normal.

Exemptions

7.6 We consider whether we can rely on an exemption on a case-by-case basis.

7.7 Where appropriate, we carefully consider the extent to which the relevant UK GDPR requirements would be likely to prevent, seriously impair, or prejudice the achievement of our processing purposes.

7.8 We justify and document our reasons for relying on an exemption.

7.9 When an exemption does not apply (or no longer applies) to our processing of personal data, we comply with the UK GDPR's requirements as normal.

For clarity anything that can potentially be ruled "exempt" will be as per the ICO guidance and will be handled on a case-by-case basis by the Governance team and yourselves and in line with the guidance Right of access/subject access requests and other rights \| ICO

8.0 PROCEDURE / EMPLOYEE REQUESTS

8.1 **ALL** requests for personal information, whether made in writing or verbally, should be sent to the governance team's dedicated email address; SubjectAccess@staffsstoke.icb.nhs.uk.

8.2 The governance team will log and acknowledge the request, providing a unique reference number and ask for any relevant identification required in order to process the SAR.

8.3 If you are asked to provide information relating to a request, a request to extend the time to respond to a SAR by a further two months can be made if the request is complex or there are a number of requests from the individual (this can include other types of requests relating to individuals' rights i.e. if the individual has made a SAR, a request for erasure and a request for data portability simultaneously). You must let the governance team know within three days of receiving the request and explain why the extension is necessary so the governance team can advise the requester that an extension is required. The requester must be notified of the extension as soon as possible and within 20 working days after the date of receipt of

the original request. The notification should be specific in explaining the reasons for the extension.

8.4 The information should then be sent to the Governance team who will then check the information provided to review the information and any redactions made are correct.

8.5 A closing letter will then be drafted by the Governance team and sent with the accompanying documentation to the Caldicott Guardian for final approval and sign-off.

8.6 Requests received for medical records from patients, or their legal / other representatives will be logged and the requester will be advised where they can obtain their records.

8.7 Where an employee requests information from their personnel file, and/or emails that the ICB may hold relating to them then the information will be sent to the ICB People Team who will provide the Governance team with the information. A search may be conducted by the Health Informatics Service (HIS) to identify any emails that may be held on the server. A deadline will be provided for the information to be provided. The providers of the information should review the information and make any necessary redactions required in conjunction with the Governance team, to allow release of the information. Information relating only to the requester should be provided (please refer to section *4 What are Identifiers and factors*).

9.0 PROCEDURE / ALL AGE CONTINUING CARE/AACC APPEALS & PUPoC

Continuing Health Care Requests:

9.1 Requests relating to Continuing Health Care/All Age Continuing Care, will be received in the SAR inbox, as detailed in 8.0 Procedure / employee requests above and triaged by the Governance team. The request will then be logged by the Governance team.

9.2 Once the information has been collated this will be reviewed by the clinical team with the Governance team to ensure that any/all redactions required are identified. Redactions will then be made by either the Business Team or the Governance team (preferably the former), in line with ICB policies and procedures.

9.3 Once the documents have been reviewed the Governance team will provide a covering letter and send to the Caldicott Guardians for final check and approval to release the information.

9.4 Once approved by the Caldicott Guardian, the Governance team will issue the information to the requester.

AACC Appeals & PUPoC

9.5 Requests will go to the SAR inbox for logging by Governance team.

9.6 The Governance team will advise the SAR number.

9.7 The Appeals & PUPOC team will collate the information, and then carry out the process in line with Procedure / employee requests detailed above.

9.8 The Appeals & PUPOC team will then issue the information to the requester.

Note Caldicott Guardian signs off all public and staff Subject Access Requests, including appeals.

APPENDIX A – SUBJECT ACCESS PROCESS MAP FOR INTERNAL AND EXTERNAL REQUESTS

Subject Access Request
Standard Operating Procedure – short version
Please refer to full Operating Procedure for full details

Request Received

- Request received into SAR inbox; subjectaccess@staffsstoke.icb.nhs.uk
- Log and acknowledge within three working days
- If information held, the Governance team will request required ID from the requester, if not already provided.
- When ID received the request to be passed to appropriate team for collation of the information from the data source.
- If information not held, the requester to be notified and advised where to obtain the information from.

Identity Checked

- Staff—Access to information contained in personnel file; ask applicant to complete a SARs request form detailing information required.
- Member of the Public—complete identify check, requiring two forms of ID; one photographic and one confirming address.

Seek Information

- Member of the Public—Seek information from the relevant department.
- Staff—Pass to HR for collation of the information.

Caldicott Guardian

- Provider of information to identify exemptions/redactions with the Governance team, where appropriate
- Send documents and covering letter to Caldicott Guardian for final check and approval for sign off;
- Chief Nursing and Therapies Officer,
- Assistant Chief Nursing & Therapies Officer, or
- Director of Nursing – Quality Assurance and Improvement

Send Information

- Once approval is received from the Caldicott Guardian, send information by requester's preferred route/method.

Note: Caldicott Guardian signs off all public and staff Subject Access Requests, including appeals.