

# Subject Access Request (SAR) Procedure

<b>Approval date:</b>	<b>14 November 2023</b>
<b>Version number:</b>	<b>2.0</b>
<b>Author:</b>	<b>Sam Collier-Sewell, Information Governance Manager and Deputy Data Protection Officer</b>
<b>Review date:</b>	<b>14 November 2026</b>
<b>Security classification:</b>	<b>OFFICIAL – Green: unclassified information</b>

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: HRPRO014

## NHS Shetland Document Development Coversheet\*

<b>Name of document</b>	Subject Access Request (SAR) procedure		
<b>Registration reference number</b>	HRPRO014	<b>New or review?</b>	Review
<b>Author</b>	Sam Collier-Sewell, Information Governance Manager and Deputy Data Protection Officer		
<b>Information Asset Owner</b>	David Morgan, Head of Information Governance, Data Protection Officer and FOI Lead		
<b>Executive lead</b>	Lorraine Hall, Director of Human Resources and Support Services		
<b>Review date</b>	14 November 2026		
<b>Security classification</b>	OFFICIAL – Green: unclassified information		

<b>Proposed groups to present document to:</b>		
IGSG (now IGG)	CCPGC	
IGT	eISG (now DGG)	

Date	Version	Group	Reason	Outcome
10/09/19	0.1	IGSG	Review of first draft	AC&R
17/09/20	0.2	IGSG	Review of second draft	PRO
06/10/20	0.2	eISG	Final approval	A
14/11/23	1.2	IGG	Final Approval	A

<b>Examples of reasons for presenting to the group</b>	<b>Examples of outcomes following meeting</b>
<ul style="list-style-type: none"> <li>Professional input required re: content (PI)</li> </ul>	<ul style="list-style-type: none"> <li>Significant changes to content required – refer to Executive Lead for guidance (SC)</li> </ul>
<ul style="list-style-type: none"> <li>Professional opinion on content (PO)</li> </ul>	<ul style="list-style-type: none"> <li>To amend content &amp; re-submit to group (AC&amp;R)</li> </ul>
<ul style="list-style-type: none"> <li>General comments/suggestions (C/S)</li> </ul>	<ul style="list-style-type: none"> <li>For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)</li> </ul>
<ul style="list-style-type: none"> <li>For information only (FIO)</li> </ul>	<ul style="list-style-type: none"> <li>Recommend proceeding to next stage (PRO)</li> </ul>
<ul style="list-style-type: none"> <li>For proofing/formatting (PF)</li> </ul>	<ul style="list-style-type: none"> <li>For upload to Intranet (INT)</li> </ul>
<ul style="list-style-type: none"> <li>Final Approval (FA)</li> </ul>	<ul style="list-style-type: none"> <li>Approved (A) or Not Approved, revisions required (NARR)</li> </ul>

**\*To be attached to the document under development/review and presented to the relevant group**

**Please record details of any changes made to the document in the table below**

Date	Record of changes made to document
22/08/19	Document created by Sam Collier, Information Governance Officer from NHS Grampian’s Procedure for Personal Data Rights Requests v3
20/08/20	Edits to content and structure made by Information Governance Team
21/10/20	Content approved by eISG. Hyperlinks, minor revisions and Level 1 & 2 forms info added. Saved as version 1.0
17/11/2020	Clarification added in sections 4.1 and 4.2 regarding checking, redaction and release of records.
15/04/2021	Minor change to text in section 7.1 made by IG Team to make it clearer that the online form should be used at the start of both level 1 & 2 SARs. Replaced ‘EEA’ with ‘UK’ in section 12. Saved as version 1.1
23/10/2023	Review by Sam Collier-Sewell in consultation with the IG Department: updated links, governance groups and formatting; added clarification on non-health records (other than employment records); removed links to paper forms and references to obsolete forms/processes. Saved as version 1.2
14/11/2023	Approved at IGG. Saved as version 2.0

## Contents

1. Purpose .....	5
2. Introduction .....	5
3. Definitions .....	5
4. Roles and responsibilities .....	6
4.1. Subject access requests – Health Records.....	6
4.2. Subject access requests – non-health records .....	7
5. Eligibility and limiting/denying access .....	7
5.1. Data about a living individual .....	7
5.2. Deceased person’s Health Record .....	7
5.3. Reasons for limiting or denying access to Health Records.....	8
5.4. Reasons for limiting or denying access to non-health records.....	8
5.5. Support with decisions about eligibility and limiting/denying access.....	8
6. Requests for rectification .....	8
7. What to do with a Subject Access Request .....	10
7.1. When receiving a Subject Access Request.....	10
7.2. When a request is passed to you from the Information Governance Department.....	11
8. Information held by the Shetland Islands Council and/or Integration Joint Board .....	12
9. Proof of identity .....	13
10. Timescales.....	14
11. Release of records.....	14
11.1. Collection and sending of records.....	14
12. Content of Responses .....	15
13. Exemptions from the Right of Access and grounds for refusal .....	16
14. Complaints.....	16

## 1. Purpose

This document replaces the Access to Health Records Procedure and sets out NHS Shetland procedures for compliance with requests by individuals to exercise their rights over their own personal data under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The document also covers requests for access to a deceased person's health records under the Access to Health Records Act 1990 (AHRA).

This document should be read in conjunction with:

- Information Governance Policy
- Records Management Policy
- Data Protection Policy – in development

## 2. Introduction

Any person, or their authorised representative, has the right to apply for access to the personal data (including both health records and non-health records, such as staff records) which NHS Shetland holds about them and to receive a copy free of charge. This process is called Subject Access and the application is called a Subject Access Request or SAR.

Under the Access to Health Records Act 1990 applications for access to a deceased patient's health record may be made, usually by the patient's personal representative or any person who may have a claim arising out of the patient's death.

Any person also has the right to have inaccurate personal data relating to them corrected. This is known as the right to rectification.

In certain circumstances, individuals may also have the right to object to NHS Shetland's use of their data, to restrict its use, or to have personal data erased.

For more information see <https://ico.org.uk/your-data-matters/>

## 3. Definitions

A **Subject Access Request** is a request made by an individual for access to, or a copy of, their own personal data. The request does not need to state that it is a Subject Access Request or refer to data protection law. See [Section 7.1](#) for more detail. The term Data Subject Access Request (DSAR) is also used.

The **Data Subject** is the individual to whom personal data relates and who may exercise a range of rights over those data.

A **Health Professional** is a registered clinician (including AHPs) with knowledge of the healthcare provided to the data subject.

The **Appointed Manager** is a member of staff in the clinical/organisational area relevant to the request

A **Health Record** is any record which consists of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.

An **Employment Record** contains an employee's employment history, performance and management records including appraisals, leave records and any procedures recorded.

## **4. Roles and responsibilities**

The Data Protection Officer (DPO) is responsible for maintaining and updating this procedure.

The Feedback and Complaints Officer is responsible for the handling of complaints relating to subject access requests.

The Information Governance Department is responsible for:

- Ensuring the logging of all requests
- Confirming the consent of the data subject if someone else claims to be applying on their behalf
- Confirming the identity of the data subject and applicant
- Liaising with Finance department where fees are chargeable for further copies of information already provided under a SAR
- Forwarding the request to the relevant department
- Monitoring the progress of requests
- Escalating issues to the appropriate line manager to ensure compliance with mandatory timescales
- Providing audit reports to the Information Governance Group (IGG)
- Providing advice and support to Health Professionals and Appointed Managers

### **4.1. Subject access requests – Health Records**

The Appointed Manager is responsible for:

- Checking that access should be granted. Access can usually only be denied or restricted for the reasons specified in Section 5.3
- Ensuring that relevant Health Professionals have checked the patient's health records
- Arranging for applicant to view the relevant records
- Providing copies of the relevant parts of the record
- Agreeing with Information Governance Department how the information for each SAR will be collated and released

The Health Professional is responsible for:

- Alerting the Appointed Manager and/or Caldicott Guardian to any potential grounds for denying or restricting access to the health record requested (see Section 5.3)
- Protecting the personal data of third parties identified in a health record (e.g. by redaction)
- Completing the DSAR Assessment to confirm that the records requested have been checked, redacted as necessary and authorised for release.

## 4.2. Subject access requests – non-health records

The Appointed Manager is responsible for:

- Checking that access should be granted. This can usually only be denied in the circumstances described in Section 5.4
- Ensuring that the record has been checked and that the personal data of third parties identified in the record are protected (e.g. by redaction)
- Arranging for applicant to view the relevant records
- Providing copies of the relevant parts of the record
- Providing relevant contextual information
- Agreeing with Information Governance Department how the information for each SAR will be collated and released
- Completing the DSAR Assessment to confirm that the records requested have been checked, redacted as necessary and authorised for release.

## 5. Eligibility and limiting/denying access

### 5.1. Data about a living individual

A subject access request can be made by any of the following:

- The data subject; this can be a patient, employee, former employee or member of the public
- A solicitor or representative of the individual, provided consent is given
- Any person with parental responsibility for a child under 12 years of age
- Any person with parental responsibility for a child under 16 years of age, if the child person has consented, or lacks capacity to provide such consent
- An agent or attorney appointed by a court to manage the property and affairs of an individual who lacks capacity to manage their own affairs

Note that the right of access to an individual's data **always** rests with that individual, the data subject. When an authorised third party (for example a solicitor or parent) requests information, they are exercising the **data subject's** right to access, not their own.

### 5.2. Deceased person's Health Record

A request for a deceased patient's record can be made by:

- The patient's representative
- Any person who may have a claim arising out of the patient's death.

Requests for such records may also be made by other individuals, such as relatives of the deceased patient. Such requests must be considered on a case-by-case basis.

### **5.3. Reasons for limiting or denying access to Health Records**

There are certain circumstances in which NHS Shetland can limit or deny access to a Health Record:

- Where the release of the requested information may cause serious harm to the physical or mental health or condition of the data subject, or any other person. Assessing whether or not this is the case is known as the Serious Harm Test.

The Serious Harm Test is carried out by the Caldicott Guardian (or designated deputy) with the support of relevant health professionals

- Where access would disclose information relating to a third person who has not consented to that disclosure. This does not include health professionals involved in the data subject's care.
- When someone requests access to health data about a child under 16 for whom they have parental responsibility and the disclosure is against that child's expectations or expressed wishes
- When someone requests access to the health record of a person for whom they are acting under legal authority (e.g. under power of attorney or as the executor of a deceased patient's estate) and the disclosure is against that person's expectations or expressed wishes

### **5.4. Reasons for limiting or denying access to non-health records**

There are certain circumstances in which NHS Shetland can limit or deny access to a non-health record:

- Where the personal information consists of confidential references
- Where access would disclose information relating to a third person who has not consented to that disclosure and where disclosure without consent would not be reasonable
- Where the personal information is processed for the purpose of management planning or forecasts and if the disclosure of information is likely to prejudice the conduct of this business or activity
- Where the personal data relates to negotiations with the individual and if the disclosure of information is likely to prejudice those negotiations

### **5.5. Support with decisions about eligibility and limiting/denying access**

Questions about eligibility and access to records can be complex. Please contact the DPO, Caldicott Guardian or Information Governance Department if you require support.

## **6. Requests for rectification**

Requests for rectification which are non-contentious (such as updates to contact details, corrections to simple facts) may be carried out as business-as-usual (BAU) by the department/service, following any relevant local protocols for amending or correcting records.

Any contentious request for rectification (such as disputed versions of events or contradictory records) must be forwarded to the Information Governance Department.





## 7. What to do with a Subject Access Request

### 7.1. When receiving a Subject Access Request

A Subject Access Request is any request for information about the data subject. **It is important to note that requests do not need to be in writing**; verbal requests should be processed in the same way as written requests. A written request can also take several forms, including letters, emails, text or social media messages, or one of the [NHS Shetland Subject Access Request Forms](#).

Requests can be as complex as asking for all the information that NHS Shetland holds about the data subject, or as simple as a request for a copy of blood test results. For clarity and to reduce the time needed to process simple requests, NHS Shetland has established two levels of SAR:

- Level 1 SARs are those where:
  - The identity of data subject and/or applicant can be verified by person receiving request (e.g. a data subject who is known to GP reception staff).
  - There is no question over the applicant's authority to access information requested
  - The information requested is limited in scope (e.g. copy of blood test results or x-ray)
  - The information requested does not contain third party personal data

For Level 1 requests NHS Shetland only needs to record basic information (Name, CHI, information requested, department, date requested, date fulfilled). This should be done by completing the [online form](#).

- Level 2 SARs are those where
  - The identity of data subject and/or applicant needs to be verified
  - There is any question over the applicant's authority to access the information requested
  - The information requested is substantial or complex
  - The information requested contains third party personal data which needs to be reviewed and/or redacted

All Level 2 requests for access to personal information; all objections to the use of personal data; and all requests for erasure, restriction or portability of personal data, must be directed to the Information Governance Department without delay. This should be done by completing the [online form](#).

While we encourage use of one of the [NHS Shetland Subject Access Request Forms](#) for Level 2 requests, NHS Shetland cannot insist on this.

NHS Shetland staff may find it useful to refer to the relevant Subject Access Request Form in order to understand and inform the applicant about what kind of information / proof of identification is required for their particular request.

Any documentation relating to a SAR must be **date stamped** and sent to the address below:

Information Governance  
Alexandra Building  
Esplanade  
LERWICK  
Shetland  
ZE1 0LL

Or by email to: [shet.dpo@nhs.scot](mailto:shet.dpo@nhs.scot)

The Information Governance Department will then forward the request to the relevant department(s).

For advice on anything related to accessing personal information, contact the Information Governance Department on:

Telephone: 01595 743015

Email: [shet.dpo@nhs.scot](mailto:shet.dpo@nhs.scot)

## **7.2. When a request is passed to you from the Information Governance Department**

Please refer to Section 4 for information on staff roles and responsibilities in the management of a SAR.

When the Information Governance Department send you a SAR, they will include a note of the due date and any other necessary information.

Please notify the Information Governance Department as soon as possible if you have any questions or require any clarification of the request.

It is important that everyone involved in searching for or preparing information in order to comply with a SAR is aware of the following:

**Under the DPA 2018, it is a criminal offence to “alter, deface, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information” which would have been disclosed under a SAR, unless such amendments would have been carried out in the normal processing of data.**

## **8. Information held by the Shetland Islands Council and/or Integration Joint Board**

Health and social care information can be held by NHS Shetland and/or the Shetland Islands Council (SIC).

The Integration Joint Board (IJB) is a data controller for the personal information it holds for the business of commissioning health and social care services from NHS Shetland and the SIC. This is primarily information about staff who fulfil IJB roles and functions.

For requests that may include personal information for which the Shetland Islands Council (SIC) and/or the Integration Joint Board (IJB) is the data controller:

- NHS Shetland will process information for which it is data controller
- NHS Shetland will notify the data subject / applicant about any data held by SIC or IJB and offer to pass their request to SIC and/or IJB for them to make direct contact with data subject / applicant. NHS Shetland will record the data subject / applicant's decision about contacting the SIC and/or IJB and progress the SAR accordingly
- If the data subject / applicant has agreed, NHS Shetland will pass the necessary details of the SAR to the SIC and/or IJB. Thereafter the SIC and/or IJB will communicate directly with the data subject / applicant in relation to relevant part of the SAR

## 9. Proof of identity

Due to the sensitive nature of the personal information NHS Shetland holds, it is essential that NHS Shetland establishes both the identity of the applicant and that they have the authority to access the information they are requesting.

In some cases the identity of the data subject / applicant will not need to be formally verified, because the individual is well known to the member of staff receiving the request. **In all other cases**, formal verification of the data subject / applicant's identity is necessary.

When a request is made on behalf of another person, the identity of both the data subject and applicant need to be verified and the authority of the applicant to act on behalf of the data subject must also be established. It is important to note that even when the applicant is known to NHS Shetland staff, it is still necessary to establish that the applicant has authority to act on behalf of the data subject.

The table below is not exhaustive, but gives an outline of the types of proofs of identity or authority that may be required:

Type of application	Proof of identity or authority required
Individual applying for their own records	1. Two forms of identification: one photographic ID, e.g. passport, driving license, and one proof of address, e.g. utility bill, council tax bill, benefits letter / book, bank statement
Application from a representative on behalf of an individual	2. As item 1 above for both the applicant and data subject.
Application from a solicitor on behalf of an individual	3. An appropriate mandate (e.g. BMA) signed by the patient
Application from a person with parental responsibility applying on behalf of their child.	4. As item 1 above for the person with parental responsibility along with the child's birth certificate or passport

With requests for deceased patients' records under the Access to Health Records Act 1990, the following applies:

Type of application	Proof of identity or authority required
Application from patient's personal representative, executor or administrator.	5. As item 1 above along with confirmation of appointment as personal representative, executor or administrator
Person making a claim arising from the patient's death.	6. As item 1 above along with details of the claim

## 10. Timescales

NHS Shetland must comply promptly with SARs and requests for rectification and, at the latest, fulfil the request or explain why we cannot do so, within one calendar month. The Information Commissioner's Office (ICO) has provided the following clarification:

“You should calculate the time limit from the day you receive the request (whether it is a working day or not) until the corresponding calendar date in the next month.”

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/#responding>

Because of this short time limit, it is essential that the date of receipt of the request is recorded and that the Information Governance Department is notified about any requests without delay.

If further information is required to confirm the identity of the applicant, NHS Shetland must let the applicant know as soon as possible. The time period for responding to the request begins once this information has been received.

In cases where it will not be possible to respond within one month, the Information Governance Department must be informed as soon as possible and **no later than 14 days** from receipt of the request, so that the Information Governance Department can advise whether an extension of up to two further months may be permitted.

Where a request is for access to a deceased patient's record which has been created or added to in the 40 days prior to the date of the request, the requested information must be released within 21 days. Otherwise, the requested information must be released within 40 days.

## 11. Release of records

Before releasing information in response to a SAR, the Appointed Manager must ensure that Sections 4 and 5 of this procedure have been applied and/or followed.

### 11.1. Collection and sending of records

The data subject / applicant can request that information is provided in a format of their choice e.g. paper copies, electronic file. Irrespective of the method requested, NHS Shetland must ensure that personal data is managed securely at all times and in accordance with NHS Shetland policies and procedures; this includes sending information in response to a SAR.

Please note that photocopying and posting paper records uses more energy and resources than emailing an electronic file. Because of this, NHS Shetland would encourage the use of secure electronic means to send copies of records.

## 12. Content of Responses

All NHS Shetland responses to SARs must include a clear description of the applicant's right to seek redress through the courts and to complain to the Information Commissioner by the following means:

Telephone: 0303 123 113

Through their online tool for reporting concerns: <https://ico.org.uk/concerns/>

or by writing to:

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

In addition, responses to Subject Access Requests must include a description of:

- The purposes for which the personal data are processed and the categories of data involved
- The sources of data (if not the data subject) and people and/or organisations with whom NHS Shetland has shared the data
- How long the data will be retained
- The other rights which data subjects have, such as rectification
- If relevant, details of any profiling use of the data and of transfers outside the UK

Where appropriate, this information may be provided in the form of a link to the relevant NHS Shetland privacy notice.

### 13. Exemptions from the Right of Access and grounds for refusal

Section 5.3 gives details of the reasons that NHS Shetland can restrict or deny access to personal information. The most commonly encountered exemptions relating to access to records are:

- Where it is deemed that the disclosure of information would cause serious harm to the physical or mental state of the applicant or to any other person – the Serious Harm Test
- Where personal information of a third party is included, consent of that person has not been given and disclosure would not be reasonable

NHS Shetland can also refuse to comply with a request if we can demonstrate that the request is manifestly unfounded or excessive.

Where information is withheld, NHS Shetland may advise the applicant of the grounds on which the information has been withheld: However, we are not obliged to do so. If it is likely to cause undue distress, NHS Shetland will not volunteer the fact that information has been withheld.

Exemptions or refusals must only be applied with the advice of the DPO and/or Caldicott Guardian. More guidance on exemptions and refusal can be found on the [ICO website](#).

### 14. Complaints

Applicants may pursue a complaint following the [NHS Shetland Complaints Handling Procedure](#), in an attempt to resolve any issue regarding refusal to comply with a request or disputed accuracy of information. Where the complaint relates to content of a Health Record, a discussion with the relevant health professional will be arranged.

Should an applicant seek to correct information they believe to be inaccurate in a health record and where it is not appropriate to comply with the request, a note must be made to reflect the applicant's view in the health record. Contact the Information Governance Department for further advice if an individual seeks to amend recorded information.

Data subjects also have the right to complain to the Information Commissioner (see details at [section 12](#) above).

Data protection law also permits redress through the courts, including the payment of compensation, and the applicant may wish to seek independent legal advice.