Western Isles Health Board

Policy Document

Title: Access to Health Records

Version 2.1

Author	Carol Macdonald, Information Governance Manager

Date of issue	IGSG approval	Next review due date	Reviewers/review team
April 2021	April 2021	April 2024	IGSG/CMT

Document Control

Version	Date	Latest changes made by	Status	Reason for change and reviewers
Version 1 Draft 1	12/10/2018	Carol Macdonald	Draft	New Policy Document
Version 1 Draft 2		Maggie Watts	Draft	Caldicott Guardian and Chair of IGSG
Version 2 Draft 1	11/11/2020	Carol Macdonald	Draft	Update
Version 2.0	15/12/2020	Carol Macdonald	Draft	Updated content and to IGSG for review in Jan 2020
Version 2.1	01/04/2021	Carol Macdonald	Draft for Approval	With amendments received from IGSG

Document Approval – Name(s) of the Individual(s) representing the Approving Committee(s)/Group(s)

Reviewers Name	Reviewers Role	Review Date
IGSG	Information	December 2018
CMT	Oversight and Approval	January 2019
IGSG	Information	January 2021
IGSG	Information	April 2021
CMT	Oversight and Approval	August 2021

CONTENTS

1 Introduction

The General Data Protection Regulation 2018 (GDPR) allows all living individuals (or an authorised representative) the right of access to their personal data. In January 2021, the GDPR was replaced with the UK GDPR to be read alongside the UK Data Protection Act 2018 (DPA 18), along with the Common Law Duty of Confidentiality and the Privacy and Electronic Communication Regulations (PECR).

The right of access, commonly referred to as a subject access request (SAR), gives individuals the right to obtain access to or to a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why their data is being used, and that it is being used lawfully.

Personal information held by NHSWI includes, but is not limited to, Health Records, Occupational Health Records, Payroll Records, Personnel Files, Corporate Records, Complaints and Incidents.

2 Legal Obligation

Article 15 of the UK GDPR states individuals have the right of access to any information held about them, of which they are the subject.

Article 15 of the UK GDPR permits a Data Subject (the person to whom the personal data relates) or someone who has been appointed by that individual, (for example a Solicitor or Power of Attorney), a right of access to personal data held and to have communicated to him/her in an intelligible form including:

i) What kind of information we keep;
ii) The reason we keep it and how it is used;
iii) How long we will keep the information or the criteria used to determine that period;
v) Who we might share the information with, and who might see your information;
vi) Any security measures we take to protect personal information sent outside Europe;
vii) The right to lodge a complaint with the ICO; and
viii) What rights exist in regard to rectification, erasure, objection or restriction of their personal data.

Data Protection legislation relates to living individuals only. For access to records pertaining to a deceased person, any family member/next of kin/representative with a claim on the deceased's estate can request access to information under the Access to Health Records Act 1990.

A subject access request relates to data held at the time the request was received. It is not acceptable to amend or delete data if you would not otherwise have done so. Under the UK DPA 2018, it is an offence to make any amendment with the intention of preventing its disclosure.

In order to comply with Caldicott Principles, only the minimum amount of information necessary must be released.

3 Procedure

An individual can make a SAR verbally or in writing, including via email, website or social media. They can make it to any part of your organisation and they do not have to direct it to a specific person or contact point. The organisational contact must direct the request to wi.infogov-wihb@nhs.scot.

Where appropriate, a patient may be informally shown their records by a health professional involved in their care, but this must not breach any of the provisions of the Data Protection Act.

A request may be made verbally, but contact by the individual in writing to confirm identity is likely. The nature of the request can make a difference to the process that is followed. The most common types of request are from:

- The data subject (the patient in the case of medical record access requests)
- A family member or the Next of Kin
- A solicitor or Insurance company acting on behalf of the subject
- The Police
- The Procurator Fiscal
- The Courts.

In addition, there may occasionally be requests from other organisations such as the Pensions Agency or NHS Counter Fraud Services. The exact process followed, however, and the time limits in which to respond will be determined on a case by case basis, depending on the requirements.

All requests that are received will be recorded in the Data Protection Database. A summary of requests made, including volume, nature of request (originator category) and time taken to respond, will be submitted to the Information Governance Steering Group on a triannual basis.

A request does not have to include the phrase 'subject access request' or reference the Data Protection Act as long as it is clear that the individual is asking for their own personal data. Although not compulsory, requests are encouraged through a SAR form, so they can be logged and processed promptly.

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.

3.1 Information to be released

NHSWI will satisfy itself that the applicant is either the data subject, or if the applicant is applying on behalf of a data subject, that the person has been authorised to do so. In the case of requests for records pertaining to children, the controller should satisfy themselves that the applicant is legally authorised to do so. The applicant will be given the SAR form to complete in order to confirm and provide evidence that they are authorised to access the records/data as requested.

If the requester simply requires to view the health record, a letter will be sent to the requester asking them to arrange a suitable time for viewing. A confirmation letter will be sent to the requester advising the date and time of the viewing along with any other necessary information.

Individuals are entitled to access to any information recorded in any format. This could be on paper, audio, electronic systems, images, x-rays, lab results, emails etc.

There are documented retention and deletion policies relating to the personal information the organisation holds, which follow the Scottish Government Records Code of Practice. Different retention periods apply to different classes of information, depending on the purpose for which it is held. Example retention periods adopted by NHS Western Isles:

- Adult general hospital records are retained for 6 years after date of last entry;
- Maternity are retained for 25 years after date of last entry;
- Children and young people's records are retained until the patient's 25th birthday; and
- Mental Health records are retained for 20 years after date of last contact.

3.2 Partial Exclusions

Responding to a SAR may involve providing information that relates both to the individual making the request and to another individual.

The UK DPA 2018 states the Board does not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the Board must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights.

For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

Generally speaking, third party references to staff members or family members are routinely documented in clinical notes, and would not normally be redacted for the purposes of a SAR. Any information recorded in clinical notes should be factual, as far as possible and only referencing third parties where pertinent to the care/record.

Any information which, on disclosure, could cause significant harm or distress to the subject or the requestor may be removed/redacted. This will be decided by the Caldicott Guardian who signs off all requests prior to disclosure, and can be supported by any information passed on by the relevant clinical teams.

3.3 Exclusions

3.3.1 Can we refuse to comply with a request?

If an exemption applies, you can refuse to comply with a SAR (wholly or partially). Not all exemptions apply in the same way and you should look at each exemption carefully to see how it applies to a particular request.

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

What does manifestly unfounded mean?
A request may be manifestly unfounded if:

The individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or

The request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual:
- explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- makes unsubstantiated accusations against you or specific employees which are clearly prompted by malice;
- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.

If you refuse to comply with a request, you must inform the individual of:
- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through the courts.

If you believe a request is manifestly unfounded or excessive, you must be able to demonstrate this to the individual.

What does manifestly excessive mean?
To determine whether a request is manifestly excessive you need to consider whether it is clearly or obviously unreasonable. You should base this on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.

This will mean taking into account all the circumstances of the request, including:

- the nature of the requested information;
- the context of the request, and the relationship between you and the individual;
- whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the individual;
- your available resources;
- whether the request largely repeats previous requests and a reasonable interval hasn't elapsed; or
- whether it overlaps with other requests (although if it relates to a completely separate set of information it is unlikely to be excessive).

A request is not necessarily excessive just because the individual requests a large amount of information. As stated above, you must consider all the circumstances of the request.

3.3.2 Other Exclusions

Some exemptions apply because of the nature of the personal data in question, e.g. information contained in a confidential reference. Others apply because disclosure of the information is likely to prejudice your purpose, i.e. it would have a damaging or detrimental effect on the individual, or on what you are doing.

Legal Privilege
The Scottish law concept of confidentiality of communications provides protection for both communications about the obtaining or providing of legal advice and communications made in connection with legal proceedings.

Legal professional privilege is only available for communications that are:
- confidential in nature;
- except where litigation is in contemplation, made solely between client and professional legal adviser acting in a professional capacity; and
- made for the dominant purpose of obtaining or providing legal advice or being used by lawyers in possible or probable litigation.

A communication is a document that conveys information and it can take any form, including a letter, report, email, memo, photograph, note of a conversation or an audio or visual recording. It can also include draft documents prepared, e.g. with the intention of putting them before a legal adviser.

Freedom of Information
You may receive a SAR in the form of a Freedom of Information request. If it is clear that the requester is merely asking for their own personal data, but they have cited FOISA, you should do the following.

- Deal with the request as a SAR in the normal way. The requester does not need to make a new request. You may need to ask the individual to verify their identity.
- Under FOISA, personal data disclosure is exempt and must be dealt with as a SAR.
- It is good practice for public authorities to clarify within 20 working days (the time limit for responding to FOI requests) that the request is being dealt with as a SAR under the DPA, and that the 30 day time limit for responding applies.

If you refuse to comply with a request, you must inform the individual of:

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through the courts.

If you believe a request is manifestly unfounded or excessive, you must be able to demonstrate this to the individual.

Publicly available information:
If an enactment requires an organisation to make information available to the public, any personal data included in it is exempt from the right of subject access.

Crime and taxation
Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes are:

- the prevention or detection of crime;
- the capture or prosecution of offenders; and
- the assessment or collection of tax or duty.

In the case of personal data consisting of information about the physical or mental health or condition of the data subject (i.e. most information held by NHS bodies) the Data Protection (Subject Access Modification) (Health) Order 2000 provides exemptions from the subject access rights in two situations:

- Where permitting access to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person (which may include a health professional).

- Where the request for access is made by another on behalf of the data subject, such as a parent for a child, access can be refused if the data subject had either provided the information in the expectation that it would not be disclosed to the applicant or had indicated that it should not be so disclosed, or if the data was obtained as a result of any examination or investigation to which the data subject consented on the basis that information would not be so disclosed.

3.4 Alterations – Misfiles/missing (Datix)

As part of the processing of SARs, the information will be overseen by the Information Governance Manager and the Caldicott Guardian, before being issued. This is to ensure the information relates to the individual requesting, and that no third party references or information is present that should not exist within the record, that the information is complete and up to date. Any misfiles or information found to be missing is recorded internally on the Datix Incident Management Reporting system, and investigated and dealt with by the appropriate department.

3.5 Request from Data Subject

3.5.1 Clarification

If a requester asks for ‘all the information you hold’ about them, they are entitled to do that. If you process a large amount of information about an individual, you may ask them to clarify specifics about the requested information to allow a reasonable search of their records.

You should ensure the process of seeking and obtaining clarification is quick and easy for the individual, and as far as possible you should provide advice and assistance to help them clarify their request. You should explain that the clock stops from the date that you request clarification and will resume once the individual responds. You should also specify whether the individual needs to reply by a certain time.

Where you seek clarification, but do not receive a response, you should wait for a reasonable period of time before considering the request ‘closed’. While one month is generally reasonable, you should adopt a proportionate and reasoned approach.

If you need to request both clarification and proof of ID, you should do so as soon as possible.

You may be able to extend the time limit by two months if the request is complex or the individual has made a number of requests.

3.5.2 Identification

To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that:

- you know the identity of the requester (or the person the request is made on behalf of); and
- the data you hold relates to the individual in question (e.g. when an individual has similar identifying details to another person).

You should not request more information if the requester's identity is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

Although your organisation's policy is to verify identity by asking for a copy of a utility bill, it is unreasonable to do so in this case since you know the person making the request.

You should also not request formal identification documents unless necessary. First you should think about other reasonable and proportionate ways you can verify an individual's identity.

Whilst you do not need to keep copies of ID documents, it might be helpful to keep a note of: what ID documents the individual provided:

- the date you verified them; and
- details of who in your organisation verified them.

3.6 Request from Family Member/Next of Kin

Under the Access to Health Records Act 1990, a family member or next of kin who can provide evidence that they have a claim on the deceased's estate and/or are their legal executor, may be provided with information on the deceased.

Generally speaking, information released would cover the last episode of care only, unless there are reasons to provide additional information. Any information provided by a patient when they were alive, is deemed confidential even after death and as a result, the data should be dealt with on a case by case basis. See Access to Health Records (Deceased) Form.

3.7 Request from Third Parties

Many requests are submitted on behalf of a patient by a third party such as solicitor or insurance company instructed to work on their behalf. These agencies usually write to the Information Governance Department, detailing the data requested under the Data Protection Act, and including a signed consent to release form. These requests are logged on the SAR Database, and processed internally.

In some cases, an individual may not have the mental capacity to manage their own affairs. It is reasonable to assume that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority.

3.8 Request from Police/Procurator Fiscal

NHS Western Isles has a duty of confidentiality to the patient and also a legal requirement to release information to law enforcement agencies in certain circumstances. These are covered under Schedule 2, Part 1(2) of the Data Protection Act 2018, and relate to:

- Safeguarding National Security
- Prevention or detection of a crime
- The apprehension or prosecution of offenders
- The collection or assessment of any tax or duty.

If a request for information is received from the police it must be accompanied either by a signed consent form from the data subject or a completed 'Request for Disclosure of Personal Data' form detailing the reason that the information is required.

Requests for information, commonly in the form of copies of medical notes or reports from the police usually have a level of urgency around them. Requests of this nature, typically are directed to the Information Governance Department, contain a signed consent form from the patient/prisoner, and they are logged and processed in a shorter timescale than the usual SAR. Sometimes court dates are stated, but generally NHS Western Isles aim to release the requested information in 10 days.

Collection of the information would be in person, with a release form signed and countersigned, and ID confirmed. It could also be posted by Royal Mail Recorded Delivery, on request.

Requests from the Procurator Fiscal are unlikely to require consent from the data subject but should be related to a crime or a sudden death. These requests should be complied with as quickly as possible and in any event within 7 days. This position is supported by CEL 11 (2007).

3.9 Request for information about Children

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of 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 you are confident that the child can understand their rights, then you should usually respond directly to the child.

You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

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, you should take into account, among other things:

- 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 from agencies like the Children's Reporter are made by letter to the Information Governance Department, with the relevant legal/court documentation and processed in accordance with the timescales requested, as often there are urgencies around producing the information.

Information requested from a parent, who may not be living with the child, would also be looked at on a case by case basis. Mothers or fathers with parental rights have full entitlement to receive information pertaining to their children, unless there is a court order to the contrary.

i. Parents, or those with parental responsibility, will generally have the right to apply for access to their child's health record.

ii. The natural (birth) mother of the child and who is named on the birth certificate will normally automatically have parental responsibility.

iii. The father will have parental responsibility if he is named on the child's birth certificate (applies to births registered from 4 May 2006 onwards). If the child was born before this date then the father will have parental responsibility if he is married to the birth mother or he has an order from the Court.

iv. Where a child is considered capable of making decisions about his/her clinical treatment, the consent of the child must be sought before a person with parental responsibility can be given access to the child's health records. In Scotland this generally relates to children aged 12 years of age and over.

Good practice dictates that the child should be encouraged to involve parents or those with parental responsibility in their treatment.

Where doubt exists regarding whether the child is capable of making decisions, then advice should be sought from the child's consultant (or relevant health professional).

v. Parental responsibility may be legally revoked in the following circumstances:
   - ~ Legal changes to Fostering Arrangement or Adoption Order;
   - ~ Care Order (Local Authority). Although the parents do not lose parental responsibility, the Local Authority can put in place a Care Order which can limit the extent to which a person can exercise their parental responsibility;
   - ~ Court Residence Order; or
   - ~ Emergency Protection Order (Local Authority).

vi. If there is any doubt about the level of parental responsibility and you have received a request for information relating to a child (e.g., if the parents are separated), please contact the Data Protection Adviser for advice.

3.10 Request from Hospitals/Clinicians

When clinical areas such as radiology or labs receive routine requests for patient data from another clinician/hospital we do not tend to record these as a SAR, and they are dealt with in

house as often there is a clinical urgency around these requests. Any requests of this nature should be dealt with by the department where the data has been requested, confirming the identity of the requestor, receiving the request in writing and transferring copies of the requested information safely and securely. This should be via NHS email, password protected files, or through File Transfer Protocols (FTP) aided by our local IT department. Business as usual sharing of this nature is covered by the Intra NHS Scotland Sharing Accord.

3.11 Request from out with EU

Generally speaking, personal data will not be processed or shared outside the EU. The UK GDPR and DPA 2018 prohibits sharing personal information out with the EU without adequate security measures in place. All data sharing out with the UK will need to be assessed on a case by case basis, liaising with Data Protection authorities in each country, as appropriate.

There will be exceptional circumstances when this will be allowed. One example could be tourists returning home requiring their insurance companies to access health data. If the patient has consented, ideally in writing, data may be shared assuming we are satisfied the people are who they say they are, the information can be passed on in a secure manner (encrypted email (as theirs is not secure), password protected, recorded delivery etc. and copies or originals retained until transfer complete).

3.12 Request from External Organisations

Requests for personal information may be requested from agencies such as Disclosure Scotland, GMC, DWP, and Children's Reporter etc. These requests should be dealt with on a case by case basis. The requestor must satisfy the controller of the legal basis for the information sharing, and the controller should take advice, making all redactions, as required, before sharing any personal data.

Article 23 of the General Data Protection Regulation allows (but does not require) personal data to be disclosed to assist in the assessment or collection of any tax or duty. Any request form the Dept. of Work and Pension for access to any information held about an individual must be accompanied by the relevant form.

3.13 Timescales

Legislation states that a SAR must be processed on receipt without undue delay, and completed within one month of receipt.

Time is calculated from the day after the request is received, (whether the day after is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Requests can be extended by up to an additional 60 days, if the request is deemed complex, requires additional clarification or multiple requests have been made. NHS Western Isles will provide a clear explanation as to why this deadline might be extended in the event of a complex query.

- NHSWI will aim to acknowledge all requests for personal information within two days of receipt of request.

- NHSWI will aim to respond to requests for personal information within one calendar month as outlined in Article 14 of the UK GDPR and, wherever possible, within 21 calendar days.
- The one calendar month period will be calculated from the day the request was first received, irrespective of which person / department have first received the request within the Board.
- The one calendar month period will not commence until the Board has sufficient information to process the request.
- It is good practice to inform the requester if you cannot provide the information within the timescales explaining the reasons for this.
- Where the application does not include sufficient information to identify the person making the request or to locate the information, the one calendar month clock will stop and restart once the information has been received.
- Requests will be considered complete/closed after 3 months if the further information requested by NHSWI from the application has not been received.

3.14 Fees

From 25th May 2018, fees are no longer applicable to SARs.

Where a request is manifestly unfounded or excessive, a “reasonable fee” may be charged for the administrative costs of complying with the request.

A reasonable fee may also be charged if an individual requests further copies of their data following a request. Any fee must be based on the administrative costs of providing further copies.

4 Complaints Procedure

If you wish to complain about any aspect of the manner in which your access request was handled, in the first instance you should submit your complaint in writing to the Information Governance Manager, NHS Western Isles, 37 South Beach, Stornoway, Isle of Lewis, HS1 2BB. And if you are not satisfied with the response you receive you may refer your complaint to an independent arbiter such as the Health Service Commissioner or the Information Commissioner.

If you wish to formally complain, please contact:

Complaints Officer
NHS Western Isles
Health Board Offices
37 South Beach
Stornoway
Isle of Lewis
HS1 2BB

You can also direct any complaints to the Information Commissioners Office by contacting:

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

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

5 References

European Data Protection Regulation, formerly The Data Protection Act 1998 - https://www.gov.uk/government/collections/data-protection-act-2018

The Human Rights Act 1998 - https://www.legislation.gov.uk/ukpga/1998/42

Freedom of Information (Scotland) Act 2002 - https://www.legislation.gov.uk/asp/2002/13

Computer Misuse Act 1998 - https://www.legislation.gov.uk/ukpga/1990/18

Access to Health Records Act 1990 - https://www.legislation.gov.uk/ukpga/1990/23

Common law Duty of Confidentiality

UK GDPR

NHS Codes of Practice - https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care

NHS Western Isles - https://www.wihb.scot.nhs.uk/patient-privacy-notice

Right of Access - https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access-1-0.pdf

6 Subject Access Forms

A range of subject access forms (SARs) have been developed to enable the smooth and timeous processing of requests and information gathering, the forms we use are:

- Living - This application relates to data held in patient medical records only for living individuals (excluding records held by the GP). The Data Protection Act 2018 gives you the statutory right of access to any health record whether manual (paper) or computerised.

NHS WI Access to Health Records (Living

- Deceased - This application relates to data held in patient medical records relating to the deceased. The Access to Health Records Act 1990 gives statutory right of access to a deceased persons' health record.

NHS WI Access to Health Records (Dece

- Staff - This application relates to any personal information held by NHS Western Isles relating to you as an employee/former employee of NHS Western Isles including Human Resource Documentation, Occupational Health Information etc. (excluding records held by the GP).

NHS WI Access to Information (Staff).pdf

- Third Party/Consent - This form is to be completed when an individual is consenting to their information being released to a Third Party.

IG Data Release Form 3rd Party Select Purpc

- Police - This form is to be completed by Police Scotland when they are requesting information from NHS Western Isles

NHSWI Police Request Information -

- Electronic Search - This template is to assist in recording searches for information for compliance with the Data Protection Act 2018. It is important that records of searches for information are kept to ensure that no area is overlooked and that the data subject is provided with all the information that he/she is entitled to receive.

SAR Search Record.pdf

All these forms can be found in the Information Governance section of the intranet or by contacting the Information Governance team.

7 Issuing a Response

Before supplying any information in response to a SAR, you should also check that you have the requester's correct postal or email address (or both). If you are supplying information by fax (and we recommend that you do so only if the requester specifically asks you to), then you must ensure that you are sending it to the correct fax number. The responsibility is with the Data Controller to provide the information the individual (or their appointed representative). Any paper copies of records should be hand collected where ID is required or when specified by the requesters otherwise they should be posted Royal Mail Recorded delivery.

If an individual makes a request electronically, the information should be provided in a commonly used electronic format, unless the individual requests otherwise. If non secure email addresses are used, the NHS Mail secure method or SWAN secure file transfer should be adopted.

If you have any concerns over the method that the individual has requested you use to send their information, you should contact them, explain your concerns and ask for an alternative address or method of providing the information.