POLICY DOCUMENT

Subject Access Request Procedures Manual

2016 – Version 3.0
CS>SMT>G&R>Board

Policy Review Schedule

Date first Approved by the Board: 29 September 2012

Last Approved by the Board: January 2016

Date of Next Review: January 2018

Policy Owner: Administrative Director

Amendment Overview

Version	Date	Pages	Comments	Actioned
2012 - 1.0 (draft)	18/09/2012	25	Procedures produced and minor changes made following discussion at Governance & Risk Committee	Mark Oliver
2012 – 1.1	29/09/2012	24	Presented to the Board for approval. **Approved**. Draft watermark to be removed	Linda Craig
2012 – 1.2	24/09/2013	28	Role of NIMDTA to be included at beginning of each policy and corporate document. Footer updated to include new NIMDTA mission statement.	Linda Craig
2014 - 2.0	17/02/2014	4, 5, 22	Role of NIMDTA updated. Complaints section added to 2.13.	Mark Oliver
2014 – 2.0	25/02/2014	28	Presented to G&R Committee for approval. **Approved** subject to minor changes.	
2014 – 2.1	27/02/2014	28	Presented to NIMDTA Board for approval.	
2014 – 2.1	11/03/2014	28	Presented to Extra-Ordinary meeting of NIMDTA Board for approval. **Approved.**	
2016 – 3.0	08/01/2016	ALL	Reviewed – no changes.	Mark Oliver

2016 – 3.0	21/01/2016		Reapproved by G&R Committee.	
2016 – 3.0	26/01/2016		Reapproved by NIMDTA Board.	

Contents

Role of the Northern Ireland Medical and Dental Training Agency

The Northern Ireland Medical and Dental Training Agency (NIMDTA) is an Arm's Length Body sponsored by the Department of Health, Social Services and Public Safety (DHSSPS) to train postgraduate medical and dental professionals for Northern Ireland. NIMDTA seeks to serve the government, public and patients of Northern Ireland by providing specialist advice, listening to local needs and having the agility to respond to regional requirements.

NIMDTA commissions, promotes and oversees postgraduate medical and dental education and training throughout Northern Ireland. Its role is to attract and appoint individuals of the highest calibre to recognised training posts and programmes to ensure the provision of a highly competent medical and dental workforce with the essential skills to meet the changing needs of the population and health and social care in Northern Ireland.

NIMDTA organises and delivers the recruitment, selection and allocation of doctors and dentists to foundation, core and specialty training programmes and rigorously assesses their performance through annual review and appraisal. NIMDTA manages the quality of postgraduate medical and dental education in HSC Trusts and in general medical and dental practices through learning and development agreements, the receipt of reports, regular meetings, trainee surveys and inspection visits. It works in close partnership with local education providers to ensure that the training and supervision of trainees support the delivery of high quality safe patient care.

NIMDTA recognises and trains clinical and educational supervisors and selects, appoints, trains and develops educational leaders for foundation, core and specialty medical and dental training programmes throughout NI.

NIMDTA is accountable to the General Medical Council (GMC) for ensuring that the standards set by the GMC for medical training, educational structures and processes are achieved. The Postgraduate Medical Dean, as the 'Responsible Officer' for doctors in training, has a statutory role in making recommendations to the GMC to support the revalidation of trainees. Revalidation is the process by which the GMC confirms that doctors are up to date and fit to practice. NIMDTA also works to the standards in the COPDEND framework for the quality development of postgraduate Dental training in the UK.

NIMDTA enhances the standard and safety of patient care through the organisation and delivery of relevant and valued career development for general medical and dental practitioners and dental care professionals. It also supports the career development of general medical practitioners and the requirements for revalidation through the management and delivery of GP appraisal.

NIMDTA aims to use the resources provided to it efficiently, effectively and innovatively. NIMDTA's approach to training is that trainees, trainers and educators should put patients first, should strive for excellence and should be strongly supported in their roles.

Policy Impact

This policy may have an impact on the following:

- Data Protection Policy

Policy Influence

This policy has been influenced by the following:

- Generic Data Protection Manual produced by the DHSSPS
- Data Protection Act 1998

1. Introduction

The Data Protection Act 1998 provides clearly defined responsibilities for data controllers as to the processing of personal data. This applies to data held electronically or clerically. The Act gives data subjects the right of access to data. This applies to the Northern Ireland Medical & Dental Training Agency in respect of:

- service users and their representatives;
- staff as employees or service users

It must be remembered that all requests for personal data received are Subject Access Requests (SARs) and have the full backing of the Act. This is regardless of the type of data requested. All responses must meet the 40 calendar day deadline specified in the Act. However requests which can be covered by normal business should be dealt with as at present. Regardless of whether a request is dealt with under normal business, it must be dealt with within the 40 calendar day deadline.

2. Handling Requests

Requests for data must be considered individually. If IT & Records Management Officer (ITRMO)/Team Leaders (TLs) are in any doubt as to whether a request is a SAR, they should treat it as one. The ITRMO/TL may seek advice from the Administrative Director (AD) when making this decision.

On submission of a SAR, the data subject is entitled to:

- be told that personal data about them is being held/is not held;
- be given a description of the personal data and the purpose(s) for which the data is being held;
- be informed about the people or organisations or the sorts of people or organisations to whom the data may be disclosed;
- be told the sources of the data held;
- be provided with an intelligible copy of the data in a permanent form.

It should be assumed that the general public does not understand organisational terms such as:

- system;

- codes, abbreviations and jargon;
- and such terms should be explained in full.

The data given should normally be that held at the time the request is made. However, routine amendments and deletions of data may continue. To this extent, the data given to the customer may differ from the data that was held at the time the request was received. No non-routine amendments or deletions are permitted, nor should data be tampered with in any way in order to make it acceptable to the customer.

Some data may be exempt or legitimately withheld when responding to a SAR.

2.1 Charges

NIMDTA reserves the right to charge the recommended administrative fee, currently £10; on each occasion that access is requested

2.2 Time limits

The Act allows 40 calendar days to respond to a SAR.

This time limit is calculated from the effective date, i.e. the date the SAR is received with sufficient information to validate the identity of the person making the request.

The SAR is treated as received when it arrives with sufficient information in any location of the Organisation.

A SAR is cleared when the response is posted to the requestor.

The Organisation **must** meet the 40 calendar day deadline to comply with the Act. Data subjects are entitled to complain to the Commissioner if this deadline is missed and the Commissioner will treat such breaches seriously under the sixth Data Protection Principle.

2.3 Request for access to data

NIMDTA's policy is to make all personal data, unless covered by a specific exemption, available to individuals or their legal representatives, on request.

A valid SAR will not always take a standard form. The law states that you do not have to respond to a SAR unless you have received it in writing. However, an e-mail is admissible in this context. If a telephone request is received for data, you should ask the data subject to put the request in writing.

The letter or e-mail does not have to identify itself as a SAR, i.e. it does not have to include the words “subject access” or “Data Protection Act”. A simple request for “information you have got on me” is sufficient to be considered a SAR.

Alternatively, a SAR could be a request for a copy of one particular document.

A data controller is only obliged to respond to a request where the data subject supplies sufficient information to enable the Organisation to identify the:

- person making the request; and
- information requested.

To enable the ITRMO/TL to identify the person, the data subject may need to provide:

- their surname, previous surname if applicable, and sufficient forenames;
- their current address and any previous address if applicable;
- a reference number, e.g. National Insurance Number, staff number, pension number or other appropriate identifier;
- their date of birth.

If the ITRMO/TL has informed the data subject of the need for further information, then NIMDTA is not obliged to comply with their request until they have supplied that information. However any such request for information must be reasonable and must not be used as a delaying tactic.

2.4 Initial action on receipt of a Subject Access Request

A SAR can be received in any part of the Organisation. The person who receives the SAR must telephone the ITRMO to advise them that a SAR has been received. It must be forwarded immediately to the ITRMO. The ITRMO/TL should advise the AD of the following, by e-mail: -

- the name and contact details of the data subject making the SAR;
- the date on which it was received;
- whether confirmation or other information has been sought from the requestor;
- date the request was accepted.

Make sure all SARs are stamped with the date of receipt in the Organisation.

2.5 Confirming identity

The security requirements of the Act impose a clear responsibility on data controllers to ensure that data is not improperly disclosed. It is important therefore that false requests by persons seeking subject access to which they have no right are identified, stopped and reported. There will be occasions when it is clear that the requestor is the data subject. It will be for the ITRMO/TL to determine whether the identity of the requestor has been confirmed, this should in the first instance be based on details held by NIMDTA and information supplied in the request. If there is any doubt seek advice from the AD.

Access will normally only be given to:

- the data subject
- someone authorised by the data subject (in writing) to receive the data.

When confirming identity, maximum use should be made of:

- personal identifiers such as: -
    - name,
    - date of birth,
    - current/previous address,
- other identifiers such as:-
    - National Insurance number,
    - HSC number,
    - staff number,
    - any other identifier.

The ITRMO/TL dealing with the SAR has the discretion to seek further confirmation over and above the normal criteria if there are grounds to doubt the identity of the person requesting the personal data. Any attempted unauthorised access to information should be reported to the AD who will advise on further action.

Where a request is made by e-mail, it is particularly important to confirm the validity of the request and the identity of the person making the request. Such information can, if considered appropriate, be obtained by telephone, so long as whatever questions are asked would provide sufficient confirmation. A signed statement is not necessarily required to provide the necessary confirmation in e-mail requests.

2.6 Repeat requests

NIMDTA does not have to respond to a request when it has already responded to an identical or similar request by the same individual, unless a reasonable interval has elapsed between compliance with the previous request and the receipt of the current request.

In deciding what amounts to a reasonable interval, the following factors should be considered: the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

In cases where data changes constantly, it will be unusual to apply this criterion. In cases of doubt the ITRMO/TL must seek advice from the AD, before refusing to reply to a request.

2.7 Data subject representatives

Disclosure of data to data subject representatives should only be made where the consent of the data subject has been given in writing, unless the representative is legally empowered to act on behalf of the data subject.

If you are in any doubt about whether the representative is who they say they are, or whether consent is valid, you should not disclose the data. In all cases decisions must be made on a case by case basis.

There are certain representatives who are legally empowered to act on behalf of a data subject:

- a person given Power of Attorney (by a court or by the data subject themselves) deals with all aspects of the data subject's financial affairs. If this is the case you may disclose any data to that representative that would normally be given to the data subject.

Data cannot be disclosed to someone just because they work for a representative group such as CAB or health charities, unless the data subject has consented in writing.

Before disclosing data to anyone other than the data subject, you must be satisfied that the representative is:

- who they say they are, and
- either acting with the consent of the data subject or empowered by a Court to act for the data subject, and
- asking for relevant information.

2.8 Requests from members of staff/ex-employees

Members of staff/ex-employees of the Organisation have the same rights under the Act as members of the general public and data can be held on them both in their capacity as employees and as customers of NIMDTA.

SARs from employees/ex-employees requesting personnel details should be forwarded to the HR Department.

Requests for any other type of records should be dealt with as normal.

2.9 Exemptions

In certain circumstances, personal data does not have to be disclosed to the data subject in response to a SAR. The meaning and extent of the exemptions are not always self-evident or easy to follow, and in cases of doubt, guidance should be sought from the AD. The primary exemptions relate to:

- safeguarding national security;
- prevention or detection of crime;
- apprehension or prosecution of offenders;
- assessment or collection of tax or duty;
- personal data concerning physical or mental health;
- personal data concerning school pupils;

- personal data processed by government departments or local authorities for the purposes of social work;
- regulatory functions exercised by public “watchdogs”;
- journalistic, literary or artistic purposes;
- research, historical and statistical purposes;
- where the information is obliged to be made public under enactment;
- where disclosure is required by law or made in connection with legal proceedings, etc.;
- parliamentary privilege;
- where a claim to legal professional privilege could be maintained;
- where data is processed only for personal or family affairs.

Further detail on the exemptions can be seen in part 4 (sections 27 to 39) of the Act. Also, Schedules 7 and 8 of the Act cover the miscellaneous exemptions and transitional exemptions respectively.

The Commissioner is critical of organisations that, while withholding data legitimately, do not quote the correct sections of the Act to support their decision. Care must be taken to fully document any decision to block exempt data. In cases where the reason for non-disclosure falls under more than one section of the Act, all relevant sections must be recorded.

Once exempt data has been blocked it may be that there is very little left on the document for the data subject to read. The document must still be issued to the data subject; otherwise NIMDTA will be in breach of the Act.

If, when the exempt data is erased or blocked, it is still possible for inference to be drawn from the remaining data, insufficient data has been removed. It should not be possible for anyone to have any understanding of the data which is being withheld.

Information which was given in confidence, or bears a protective security marking, may still be disclosed. Privacy markings such as “in confidence” etc. have little effect under the terms of the Act. Whether or not such information should be disclosed depends on the content, not the endorsement.

2.10 Data relating to another/other individual

Another/other individual's data means personal data relating to any person other than the:

- data subject;
- data controller.

Another individual's data can take two forms:

- data supplied by another individual which relates to the data subject;
- details contained in the data of a data subject, which relates to someone other than the data subject.

The rule regarding disclosure of another individual's data is that the data controller is not obliged to disclose it unless:

- the other individual has consented to the disclosure to the data subject, or
- it is reasonable in all the circumstances to make the disclosure without the consent of the other individual.

The disclosure of another individual's data may result in a complaint by the other individual or the data subject to the Commissioner, if either is unhappy with the decision made. It is therefore important that all aspects are carefully considered before deciding to release or withhold another individual's data.

Each case should be considered separately. The key questions to ask before deciding whether to disclose the information or not are:

- **Has the other individual consented to the disclosure?**

  Consideration should be given to seeking consent. It may not always be appropriate to seek consent, for example if it will mean disclosing data about the data subject to the other individual.

- **Has the other individual previously given the information to the data subject making the request?**

  NIMDTA would not be justified in withholding the data in these circumstances.

- **Is the other individual's data confidential, sensitive or harmful to either the other individual or the data subject?**

  A duty of confidentiality arises in many relationships. When a clear duty of confidentiality to another individual arises, it may not be reasonable to disclose any data, which may identify that other individual.

- **Is it reasonable to disclose the data without the consent of the other individual?**

  Consideration should be given to disclosing the data without the consent of the other individual: e.g. when an employer has provided wage details. However, if the employer has requested that the source of the data be withheld, consideration will have to be given to withholding their names under section 7(6) (a).

- **Is the other individual not prepared to consent to the data being divulged to the legal representative of the data subject?**

  The other individual may be willing to consent to the data subject being given the data, but not the legal representative of the data subject. In such a case, the data relating to the other individual cannot be divulged to the legal representative. It may be appropriate to contact the data subject to advise them of this and if necessary, send the data direct to the data subject.

- **Has the other individual refused consent to the disclosure?**

  If the other individual has refused consent to disclosure of the data, then this should be taken as a strong indication that the data should not be disclosed. However, the Commissioner has advised that if consent has not been given, the data controller is still required to release the data if it is reasonable in all the circumstances.

  Reasonable is not defined, but if a clear duty of confidentiality arises disclosure of another individual's data without consent is unlikely to be reasonable. The ITRMO/TLs must consider the circumstances of each case, and make a judgement as to the confidentiality of the data.

  Any decision to disclose data without the consent of the other individual must be fully documented.

- **Does the other individual's data contain details which will identify them? If so, will blocking be sufficient to prevent the disclosure of the other individual's identity?**

  If it is decided that the other individual's data is to be blocked, disclosure of the remaining data must be made. In this situation, the person blocking the data must be positive that the other individual cannot be identified from what will be disclosed to the data subject.

2.11 Staff names

The advice from the Information Commissioner is that staff names are disclosable provided that there is no risk of harm to the staff involved. The names of staff who have already provided direct services to the person will usually already be known. With regards the disclosure of staff names, NIMDTA has a duty to consider not only the rights of the data subject, but also the rights of its staff.

If it is clear that the data subject knows the names of the staff who are included in any data and their involvement then it is reasonable to disclose their name. If not then the ITRMO/TL should inform the staff member(s) that a SAR has been received and the response will include their name.

Until case law is established, there are no clear guidelines as to when it would be regarded as reasonable to seek consent. However, it is likely in the event of a complaint from the data subject regarding non-disclosure of another individual's data, the Commissioner could regard it as reasonable to have sought consent if the member of staff still worked in NIMDTA. Conversely, it may be regarded as unreasonable to have sought consent if the member of staff had left NIMDTA and to establish contact would involve disproportionate effort. All circumstances pertaining at the time need to be taken into account.

Where consent is given, it should be recorded.

Where consent has not been sought, or has been refused, there is an obligation on NIMDTA still to consider whether it is reasonable to disclose, taking account of all the circumstances of the case. The reasons for not disclosing staff names should be documented.

It would be regarded as reasonable where the data subject is already aware of the staff member's name due to the correspondence having been sent previously to the data subject signed by the staff member, or where the customer was told the staff member's name at interview. Also, in the case of staff carrying out their normal day-to-day duties it could be reasonable not to seek consent before releasing data e.g. line manager writing annual reports, and line manager carrying out managing attendance procedures.

In all other cases (e.g. staff discipline or other contentious areas), NIMDTA considers that unless the member of staff has consented, his/her name should not be disclosed except where disclosure is necessary to the understanding of the information provided to the data subject. **All the circumstances of each individual case should be taken into account before a decision is taken not to disclose.**

The presumption of disclosure/non-disclosure of staff names must not be applied blindly, regardless of the individual circumstances of a case. **Each case should be considered on an individual basis.**

In any case where a doubt arises as to whether the staff name should be disclosed, or whether it should be disclosed if consent is not given, the AD should be consulted for advice.

2.12 Record of reasons for decision

Where it is decided that any information should be withheld and not disclosed to the data subject, the reasons and factors considered which lead to that decision should be recorded.

2.13 Enquiries following a response to a Subject Access Request

Enquiries following responses to SARs will normally fall into one of five areas:

- the data subject believes they have not received all the data held on them;
- the data subject does not understand the data;
- the data subject disputes the accuracy and/or the relevance of the data;
- the data subject finds some of the data offensive;
- the data subject is unhappy that the response was not issued within the timescales allowed.

If a data subject makes a complaint in relation to how their SAR has been dealt with and/or the response they have received, and the issue cannot be resolved locally (through the Data Protection Officer (DPO), and if necessary the Governance & Risk Committee and NIMDTA Board), the individual shall be referred to the Information Commissioner.

2.14 Documenting Subject Access Requests

The following records must be kept for each SAR :

- the initial SAR (either written format or email);
- any subsequent correspondence including e-mail and our telephone calls;
- the reasons for requesting further identity details from the data subject;
- decisions to withhold exempt data, other individuals data;

- decisions to disclose data without the consent of another individual involved;
- any other relevant information e.g. telephone calls;
- final action, to authorise the release of the reply to the data subject;
- details of the return of a SAR as not delivered and attempts to contact the data subject;
- Any advice received from e.g. AD, solicitors etc;
- Confirmation from third parties on releasing or withholding data;
- A copy of the response;
- A schedule of documents released.

Note: Make sure all details are fully documented.

2.15 Request by data subject to view/collect data at an office of the Organisation

The data subject can request that they view/collect their data from NIMDTA' office.

Data subjects must always be accompanied when viewing original documents.

2.16 Withdrawal of request for access by the data subject

There may be occasions where the data subject may withdraw the SAR, after it has been recorded in the SAR file or log.

The withdrawal of the SAR should be acknowledged in writing. Once this action has been completed, the SAR should be taken as cleared.

2.17 Requesting and monitoring requests for records

The general rule is that a TL only collates the data for their own Department.

A data subject may request data from any or all of the following:

- manual records;

- mainframe computers;
- other computers (including e-mail);
- Close Circuit Television (CCTV);
- taped conservations or their transcripts;
- still photographs;
- video recordings;
- any other systems.

2.18 Blocking/Redacting exempt or other individuals data

When blocking/redacting exempt or other individual's data, the ITRMO/TL must:

- separate those records which can and cannot be issued to the data subject;
- arrange to have all the records which can be issued to the data subject photocopied;
- ensure no deletions/amendments are made on original records;
- block any exempt data or other individual's data by using redaction tape to cover the data before making a photocopy. Alternatively if redaction tape is not available black card can be used to cover the data before a photocopy is made;
- a final check of the redacted, photocopied version of the document should be made to ensure that exempt data is properly hidden;
- arrange records in date order.

Decisions made by the ITRMO/TL to withhold data must be recorded.

2.19 ITRMO action before issuing response to Subject Access Request

On receipt of each component, ensure that:

- all data relates to the data subject;
- the correct procedures for blocking exempt data are followed;
- the correct procedures are carried out in relation to other individuals data;
- examine records for potentially offensive data;

- NIMDTA specific abbreviations have been explained;
- Any data which cannot be understood, e.g. because of poor handwriting, must be typed and a copy of the original document issued together with the typewritten transcript. If any part of the document is unreadable, this should be explained to the data subject and an apology included in the reply;
- if the latest address on any computer system differs from that on the SAR, verification of the new address is recorded;
- arrange for copying of all relevant records for issue, which includes any jacket/file cover;
- contact the AD if you have any further queries.

Ensure that the SAR file or log is updated with relevant information at the appropriate time.

This is to ensure that:

- if any action has not been carried out correctly, there will be a minimum delay in rectifying the situation;
- the management information extracted from the SAR file or log will be accurate and help identify the areas which fail to meet the deadline.

Prepare a covering letter to respond to the SAR. This will accompany the data you intend to release or not release. The letter should cover the following areas as appropriate to the particular SAR:

- a description of the personal data of which they are the data subject;
- a description of the purposes for processing the data;
- information about the people or organisations, or the sorts of people or organisations to whom you might disclose the personal data;
- information on the sources of the personal data;
- if no data has been found, indicate this to the data subject, or if none of the data can be released, state that there is no data you are required to give. There is no requirement to explain the reason for withholding or blocking data;
- an explanation of any inaccurate data being issued and details of the action the Organisation intends to take to correct the problem;
- your contact details.

2.20 Data exists but cannot be found

If it is known that data exists but cannot be found, the ITRMO/TL must ensure the Department involved acts timeously in following their guidance to trace missing documents.

If some data has been traced, continue normal action on that data.

If by the day before the 40 calendar day deadline, it is obvious that the missing data will not be found in time, then the data held by the ITRMO/TL should be issued to the data subject.

A letter should be issued to the data subject explaining what data has been found and apologising, as the full response has not been issued within the 40 calendar days, and NIMDTA has failed to meet the deadline.

When the missing action is completed and data has been traced, it should be issued to the data subject with an explanatory letter.

If, the missing data cannot be traced, the SAR file and log should be updated and a suitable explanatory letter should be issued to the data subject.

2.21 Data should exist but has been destroyed in error

If the ITRMO/TL is aware that data should exist for the data subject but has proof that it has been destroyed in error, the ITRMO/TL should write to the data subject, explaining the situation and apologising for the error.

The deadline will have been met if it is established within the 40 calendar day deadline that the data has been accidentally destroyed and either:

- that was all the data requested, or
- the other data requested had been issued within the 40 calendar days.

This must be reported to the AD.

2.22 No data held for a data subject

It may be that the Department from which the data subject has requested data does not hold anything for the data subject.

In such a case the ITRMO/TL should advise the data subject in writing or by e-mail if requested, that no data is held. The ITRMO/TL should advise the AD that the SAR has been answered.

This will advise the data subject that their SAR has been dealt with and there are no records held for them.