NHS
North Yorkshire
Clinical Commissioning Group

Subject Access Request Policy

November 2020

Authorship:	Senior Information Governance Specialist; NECS
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	November 2020
Review Date:	November 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-116
Version Number:	1.1

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Senior Information Governance Specialist	First Draft	IGSG (Nov 2020)	
0.2	Senior Information Governance Specialist	Second Draft revised for amendments from IG Steering Group		
1.0	Senior Information Governance Specialist		Approved by NHS North Yorkshire CCG Audit Committee (Nov 2020)	December 20
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

Individuals have the right under current data protection legislation subject to certain exemptions, to have access to their personal records that are held by North Yorkshire Clinical Commissioning Group (The CCG). This is known as a 'subject access request' (SAR). Requests may be received from members of staff, service users or any other individuals who the CCG has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

All SAR requests received must be forwarded to the corporate services team at nyccg.patientrelations@nhs.net

2.0 Purpose

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

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

3.0 Definitions / Explanation of Terms

3.1 Personal information

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, pseudonymised data, biometric and genetic data, and online identifiers and location data, etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition. Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.

Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary. The appropriate legal basis under Article 6 of the General Data Protection Regulation must be identified and recorded in the CCG Information Asset Register to be able to legally process personal identifiable information.

3.2 Special Category Data

Special category data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

In addition to having identified a legal basis under Article 6 of the General Data Protection Regulation to legally process personal identifiable information, to legally process special category information the CCG must identify the condition under Schedule 1 of the current Data Protection Act and the legal basis under Article 9(2) and record these on the information asset register.

3.3 Subject Access Request

A subject access request (SAR) is request made by or on behalf of an individual for the information about them, which is held by the CCG. This request does not need to be in any particular format and does not need to mention that it is a subject access request.

The Data Protection Legislation entitles all individuals to make requests for their own personal data to enable individuals to verify the lawfulness of how their information is being processed. An individual is not entitled to information relating to other people (unless they are acting on behalf of that person).

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also other restrictions on disclosing information in response to a SAR, for example where this would involve disclosing information about another individual.

3.4 Information Formats

Information can be in many forms, including (but not limited to):

- Structured record systems – paper and electronic;
- Transmission of information –e-mail, post and telephone; and
- All information systems purchased, developed and managed by/or on behalf of the organisation.

4.0 Scope of the Policy

The policy applies to NHS North Yorkshire CCG and all its employees and must be followed by all those who work for the organisation, including the Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

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

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

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

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

5.2 Caldicott Guardian/SIRO/IG Specialist

The CCG Caldicott Guardian and SIRO, and North of England Commissioning Support (NECS) IG Specialist are responsible for overseeing and advising on disclosure of individual's information held by the CCG.

5.3 Corporate Services Manager

The Corporate Services Manager is responsible for the oversight of the SAR process and administration.

5.4 Patient Relations Team

The Patient Relations Team are responsible for the administration of Subject Access Requests in line with this policy.

5.5 Line Managers

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

5.6 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy

6.0 Policy Procedural Requirements

6.1 How to recognise a Subject Access Request

In order for the CCG to action a subject access request the following must be received:

- Proof of identity of the applicant and/or the applicant representative, and proof of right of access to another person's personal information, by reasonable means (See Appendix A).
- The request must contain sufficient information to be able to locate the record or information requested.

A request does not need to be in any particular format and does not need to mention subject access request. It may be made in writing (This may be by letter, fax, email, or even social media, such as facebook or twitter). However a request may be made verbally, where this occurs ensure that a record is made of the information requested, the date requested and by whom.

It is important to note that responses to SAR requests must be returned by a secure methodology, i.e. social media must **NOT** be used to return information requested. However where the applicant is not able to make the request in writing it can be received verbally and a record of the request made on the applicants file.

All requests must be acknowledged and advised on timescales for response.

All requests must be responded to without delay and at the latest within one calendar month of receipt of the request. This time can be extended by a further 2 months where requests are complex or numerous. However if this is the case you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If the request relates to, or includes information that should not be requested by means of a SAR (e.g. it includes a request for non-personal information) then, the request must be treated accordingly, e.g. as a FOI request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under Data Protection Legislation; and another for the remaining, non-personal information made under FOI Legislation. If any of the non-personal information is environmental, this should be considered as a request made under the Environmental Information Regulations (EIR).

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

All SAR requests received must be forwarded to the corporate services team at nyccg.patientrelations@nhs.net.

Data Protection Legislation does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

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

- Where you refuse to respond you must explain to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

6.2 Assisting and advising services users in making a request

Where an individual is verbally making a request you should make a written record of the request, detailing the information they are requesting and from which service to enable its location and verify with the requestor that the record is correct.

Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request. Note some requestors may require additional assistance and therefore details might have to be supplied in an alternative accessible format, e.g. braille. Applicants can be referred to the Patient Relations Team to obtain appropriate assistance in making their application.

A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure that you and your colleagues can recognise a SAR and deal with it in appropriately and ensure it is forwarded immediately to the officer within the CCG responsible for dealing with the SAR's.

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

7.0 Requests on behalf of other individuals

7.1.1 General Third Party

A third party, e.g. solicitor may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney must be provided by the third party.

If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual who is the subject of the SAR rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

7.1.2 Requests on Behalf of Children

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

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child has the capacity to understand their rights and any implications of the disclosure of information, then child's permission should be sought to action the request.

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

The Caldicott Guardian or their nominated representative should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that, just because a child has capacity to make a SAR, that they also have capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so.

What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following should be taken into account:

- Where possible, the child's level of maturity and their ability to make decisions like this;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

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

Requests for personal information may be made by the above authorities for the following purposes:

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

A formal documented request signed a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

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

7.1.4 Court Orders

Any Court Order requiring the supply of personal information about an individual must be complied with.

7.2 Responding to Requests

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

- Date received

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

A Register has been developed by the CCG for this purpose and should be used to record the above by all those responsible for managing SAR's.

Determine whether the person's request is to be treated as a routine enquiry or as a subject access request. If you would usually deal with the request in the normal course of business, e.g. confirming appointment times or details of public meetings planned then do so.

The following are likely to be treated as formal subject access requests.

- Please send me a copy of my HR file or Medical Records.
- I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed.
- The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.

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

Ensure adequate information has been received to facilitate locating the information requested. Locate the required information from all sources and collate it ready for review by an appropriate senior manager. This review is to ensure that the information is appropriate for disclosure, i.e. to ascertain whether any exemptions apply e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed, or is information to be withheld due to on-going formal investigations. Advice may be sought from the Information Governance Team. Exemptions are detailed at Appendix B.

In the case of requests for clinical records these should be reviewed by the Caldicott Guardian or a nominated representative who shall decide to what extent data can be disclosed or whether the request is to be refused.

Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual. However if information contained within the information requested was supplied by health professionals it may be disclosed without consent if considered appropriate.

Generally the CCG must provide a copy of the information free of charge. However a 'reasonable fee' may be levied when a request is manifestly unfounded or excess,

particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact as soon as possible.

It must be determined whether the information is likely to change between receiving the request and sending the response. Routine on-going business additions and amendments may be made to the personal information after a request is received, however the information must not be altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under Data Protection Legislation.

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

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

Where it is not possible to remove third party identifiers you must consider the following.

- Has the third party consented to the disclosure?
- Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party?

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

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

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

Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:

- Crime prevention and detection, including taxation purposes,
- Negotiations with the requestor,
- Management Forecasts,
- Confidential References given by you,
- Information used in research, historical or statistical purposes; and
- Information covered by legal professional privilege.

Other exemptions are detailed at Appendix B.

If the information requested, is held by the organisation and exemptions apply then a decision must be made as to whether you inform that applicant that the information is held but is exempt from disclosure or whether you reply stating that no relevant information is held. A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing on-going or potential investigations or undue harm or distress is to be avoided. It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered.

If the information contains complex terms or codes, you must ensure that these terms and codes are explained in such a way that the information can be understood in lay terms.

7.2.1 Preparing the response:

When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case by the due date.

A copy of the information should be supplied in a format agreed with the applicant for example if the request is received electronically, then the response should be returned in an electronic format. You have one calendar month to comply with the request starting from the date you receive all the information necessary to deal with the request. It is an offence under the Data Protection Legislation and individuals can complain to the Information Commissioners Office or apply to a court if you do not respond within this time limit.

Under no circumstances should original records be sent to the applicant.

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

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

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

7.2.2 Refusing a request

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

You can also refuse to comply with a subject access request if it is:

- manifestly unfounded; or

- excessive.

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

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

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

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

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

8.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

NHS North Yorkshire CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

9.0 Consultation

This Policy has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

10.0 Training

All staff will need to be trained in recognising a SAR and who to send it to for processing on receipt.

The officers delegated with the responsibility for managing SAR's must complete appropriate training in how to deal with and record a SAR appropriately.

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment.

11.0 Monitoring Compliance with the Document

Compliance with this policy will be monitored though audits of the register of SARs received to assess to processing timescales of requests and the follow up of any complaints from applicants as a result of responses to requests.

Responsibilities for conducting monitoring.

- The IG Team will annually audit the register of SARs.
- Complaints from applicants of SARs will be investigated by the CCG with assistance from the NECS IG Team where required.

12.0 Arrangements for Review

The policy will undergo a full review every 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy

13.0 Dissemination

This policy will be published on the CCG's internet and will therefore be available to both staff and the public.

Staff will be made aware of the existence of this policy and all subsequent updates via the staff newsletter.

14.0 Associated Documentation

- Information Governance Framework and Strategy
- Data Protection and Confidentiality Policy
- Records Management Policy

15.0 References

- Data Protection Act 2018
- DoH: Guidance for Access to Health Records Requests
- Freedom of Information Act 2000

16.0 Appendices

Appendix A: Registration & Authentication Examples of Documentary Evidence

Appendix B: Subject Access Request Exemptions

17.0 Appendix A - Registration & Authentication Examples of Documentary Evidence

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

Personal identity

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

Active in the Community

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

- Record of home visit
- Confirmation from an Electoral Register search that a person of that name lives at that address
- Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed)
- Local authority tax bill (valid for current year)
- Current UK photo card driving licence (if not used for evidence of name)

- Current full UK driving licence (old version) (if not used for evidence of name)
- Bank, building society or credit union statement or passbook containing current address
- Recent original mortgage statement from a recognised lender
- Current local council rent card or tenancy agreement
- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit
- Court order

18.0 Appendix B - Subject Access Request Exemptions

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

Category	Exemption
National Security	Personal information that is held in respect of the maintenance of national security is exempt from disclosure.
Crime and Taxation	Section of the personal information contained in the records, or individual records that relate to the prevention and detection of crime or the apprehension or prosecution of offenders
Health, Education and Social Work	Health exemptions are mentioned in section 7 Social work records exemptions comes under the Data Protection (Subject Access Modification)(Social Work) Order 2000 relates to personal information used for social work purposes: Where release of information may prejudice the carrying out of social work by causing serious harm to the physical or mental condition of the data subject or others. Certain third party's information can be released if they are a "relevant person " (a list is contained in the order) as long as release of the information does not cause serious harm to the relevant person's physical or mental condition, or with the consent of the third party
Regulatory activity	Personal data processed by the PCT for the purposes of discharging it functions are exempt if the release of such information would prejudice the proper discharge of those functions.
Research, history statistics	Where the personal data is used solely for research purposes and as long as resulting statistics are not made available which identify the person.
Human fertilisation and embryology	Personal information can be withheld in certain circumstances where it relates to human fertilization and embryology.
Legal Professional Privilege	Any correspondence to or from or documentation prepared for or by the Trust's internal or external legal advisors may be exempt from disclosure and advice should always be sought relating this class of information.