

Subject Access Request Policy

Document Reference Information

Version	1.2
Status	Approved
Approving Committee	NWL Collaboration of 8 CCGs Federation Operational Committee
Author/Lead	Head of Information Governance & DPO
Date Effective	Dec 2018
Date of Next Formal Review	Dec 2019
Annual Review	June 2020 DPO (Corporate & GP)
Review	August 2020 Head of Governance/SIRO
Approving Committee	The Governing Body
Date Effective	September 2020
Date of Next Formal Review	June 2021

Version Control Record

Date	Version	Action	Amendments
November 2014	0.5	First version	Draft
July 2017	1.0	The General Data Protection Regulation (GDPR) become law May 25 th 2018 and this policy will be revised again	Editorial
Dec 2018	1.1	Revised for GDPR & Data Protection Act 2018 compliance	New legislation updates
June 2020	1.2	Annual review	GDPR updates
August 2020	1.2	Review (SIRO)	N/A

Other relevant documents to this policy:

Safeguarding Policy

Confidentiality and Data Protection Policy

Information Governance Policy

Information Governance Management Framework

Incident Reporting and Management Policy

Records Management Policy

“The NWL Collaboration of 8 CCGs incorporates and supports the Equality Act 2010 and the human rights of the individual as set out in the European Convention on Human Rights and the Human Rights Act 1998”

Version 1.2 Sept 2020

Subject Access Request Policy

Page 1 of 24

CONTENTS

Section Number	Paragraph Heading	Page Number
	Document Reference Information	1
	Version Control Record	1
1	Introduction	3
2	Scope	3
3	The Data Protection Act 2018	3
4	Access to health Records Act 1990	4
5	Roles and Responsibilities	4
6	Implementation	5
7	What's new under the GDPR and the Data Protection Act 2018?	11
8	References	11
9	Glossary	12
Appendices		
Appendix 1	Pathway to Responding to Subject Access Requests	14
Appendix 2	Subject Access Request Form	15
Appendix 3	Essential ID requirement	23
Appendix 4	Equality Impact Assessment	

1. Introduction

- 1.1 NWL Collaboration of 8 CCGs is required to ensure that it has a policy and procedure in place to respond to Subject Access Requests under the Data Protection Act 2018.
- 1.2 This policy deals with the rights of data subjects under the Data Protection Act 2018. The Act gives individuals (known as data subjects) the right, subject to certain exceptions, to see (view) and obtain a copy of all personal data about themselves that is held in either computerised or manual formats. Data subjects have access rights to all records irrespective of when they were created. To exercise this right, an individual makes a request for information where they are the subject of that information or data.

2. Scope

- 2.1 This policy applies to all requests for access to personal data held by the NWL Collaboration of 8 CCGs. This applies to anyone about whom the NWL Collaboration of 8 CCGs holds information – including staff, ex-staff, residents, service users, independent contractor suppliers, and contractors. This policy will provide a framework for the NWL Collaboration of 8 CCGs to ensure compliance with the Data Protection Act 2018 and the GDPR.

3. The Data Protection Act 2018

- 3.1 The Data Protection Act 2018 (DPA2018) regulates the processing, including the disclosure, of information about identifiable living individuals. Subject to specified exemptions the Act requires data controllers (including NHS organisations) to comply with the “data protection principles” set out in Chapter 2, sections 38-40 of the Act.
- 3.2 The Information Commissioners Office (ICO) is the UK’s independent public body that is responsible for governing Data Protection compliance: www.ico.gov.uk/
- 3.3 The DPA 2018 gives individuals (known as data subjects), or their authorised representative, the right to apply to see certain personal data held about them, including health records. These rights are known as “subject access rights”, and are contained in Chapter 3; Section 45-50 of the Act.
- 3.4 Data Protection legislation defines a health record as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.
- 3.5 A health record can be recorded in computerised or manual form or in a mixture of both. It may include such things as; hand-written clinical notes, letters to and from other health professionals, laboratory reports, radiographs and other imaging records e.g. X-rays and not just X-ray reports, printouts from monitoring equipment, photographs, videos and tape-recordings of telephone conversations.

3.6 Data Protection legislation is not confined to health records held for NHS purposes. It applies equally to all relevant records relating to living individuals; this includes the private health sector and health professionals' private practice records.

4. Access to Health Records Act 1990

4.1 The Access to Health Records Act 1990 (AHRA) regulates the processing, including the disclosure, of information about identifiable individuals that are deceased. The Act states that only two groups of people may access the patient's health records:

- the patient's representative (executor or administrator of the estate) or
- anyone with a claim arising out of the patient's death

4.2 In order to show that the Applicant has been appointed as the personal representative the NWL Collaboration of 8 CCGs will ask for a copy of the Grant of Probate or Letters of Administration. The NWL Collaboration of 8 CCGs understands that these documents are not always available so may accept requests from the next of kin providing they have proof of identity and taking into account the patient's wishes before they died. The NWL Collaboration of 8 CCGs will also consider the confidentiality principles when releasing this information.

4.3 The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.

4.4 There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the record holder should seek legal advice.

4.5 Record holders must satisfy themselves as to the identity of applicants who should provide as much information to identify themselves as possible. Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim. Personal representatives will also need to provide evidence of identity.

5. Roles and Responsibilities

5.1 The Governing Body

The Governing Body has a duty to ensure that the requirements of the Data Protection Act 2018 are upheld.

5.2 Caldicott Guardian

The Caldicott Guardian of the NWL Collaboration of 8 CCGs (Chief Nurse & Director of Quality) is responsible for ensuring that the NWL Collaboration of 8 CCGs is compliant with the confidentiality requirements of the Data Protection Act.

5.3 Subject Access Lead (**Data Protection Officer – DPO**)

In order to ensure that NWL Collaboration of 8 CCGs is able to meet the requirements of the Data Protection Act 2018/ EU GDPR and Subject Access Requests requirements consistently, the NWL Collaboration of 8 CCGs has appointed a single person to act as Data Protection Officer. .

The Data Protection Officer is responsible for:

- Overseeing the systems and procedures that support the implementation of this policy.
- **Support / Advise staff processing the subject access request in ensuring** consent is obtained from the individual for the release of their records/data, in accordance with the requirements of the Data Protection Act 2018 and NWL Collaboration of 8 CCGs Guidelines and Procedures for Subject Access Requests under the Data Protection Act 2018.
- Providing advice to nominated Directorate/departmental Leads and/or Heads of Service/Senior Managers on exemptions and exclusions under the Data Protection Act.
- Sign off the release of the requested information.

Information Governance Lead/staff is responsible for:

- Liaising with other organisations to process the access request in the event of shared records/data
- Coordinating the release of the information and ensure that sufficient identification is given by the applicant

5.4 Service Leads will be responsible for:

- Ensuring they have in place a system to respond to requests with a responsible individual identified to assist or manage the process.
- Responding to requests promptly within the agreed timescales in line with this policy
- Ensuring the record/data is reviewed by an appropriate professional and the identification of exemptions, and third party information in accordance with the Act.
- Ensuring that necessary redactions are carried out by the appropriate department/Business unit
- Approval for their release is undertaken by a senior and appropriate professional and this approval undertaken as a priority.
- Ensuring their staff are aware of this policy

5.5 All staff are obliged to adhere to the policy.

6. IMPLEMENTATION

6.1 Subject Access Requests – the rights of individuals

The GDPR and DPA 2018 ensures the transparency of data processing by obliging data controllers to explain to individuals how their data will be used (Principle 1) and by providing the right of subject access. As the “listed GDPR provisions” (in paragraph 18 of Schedule 2 to the DPA 2018) include the right to be informed (Articles 13 and 14 of the GDPR).

The Act provides that individuals who request access to their data should:

- be informed whether or not they are the subject of any data being processed by a data controller organisation; and
- Where data is being processed, be provided with an understandable copy of the information held about them on request. It should also be provided in a ‘permanent form’ unless the provision of the information in a permanent form would involve ‘disproportionate effort’.

Individuals also have the right to:

- a description of the personal data of which they are the data subject;
- a description of the purposes for which the data are being processed or are to be processed – this could be based on the information supplied to the Commissioner’s office during notification or on some information specific to the applicant;
- a description of the recipients of the data;
- any information available to an organisation on the source of the applicant’s data; and;
- where the applicant specifically requests it, the logic involved in any fully automated decision-taking that has or may have a significant effect on the individual concerned, such as a decision in relation to credit worthiness (except where the logic would constitute a trade secret).

6.2 Subject access requests from patients

Where a patient is unable to manage his/her own affairs then NWL Collaboration of 8 CCGs will only accept an application by a person appointed by the Courts e.g. Under the Court of Protection (or acting within the terms of a registered Enduring Power of Attorney). For further guidance, see the Mental Capacity Act.

A young person over 13 years of age, but under 18, or a child under 13 who is considered to be Fraser competent (see DOH 'Best practice guidance for doctors and other health professionals on the provision of advice and treatment to young people under 16 on contraception, sexual and reproductive health' 2004) may exercise their right of access to his/her health records under the Act. The person with parental responsibility also has a right of access to the records.

However, NWL Collaboration of 8 CCGs must be particularly careful to verify that the young person has either initiated such a request or consented to such a request being made or that the young person's lack of understanding requires a parent or guardian to act on their behalf. Another important aspect may well be the nature of the personal information may contain reference to the parent or guardian within the young person's records: for example, where allegations of abuse have been made against the parent or guardian in social work file. NWL Collaboration of 8 CCGs will need to handle requests from minors carefully; consideration needs to be given to balancing the harm that might arise against the possible benefits of supplying the information and will involve NWL Collaboration of CCG's Designated Professionals in all such requests.

When an applicant is not able to produce a written consent from the patient to access the patient information or is not able to evidence that he/she is entitled to access the patient information, NWL Collaboration of 8 CCGs will request further information from the applicant on the reason for the request to decide whether it would be justifiable to release the information to the applicant in any event.

6.3 Data identifying a Third party

Where personal data relating to the applicant also identifies another individual, the applicant's right of access must be weighed against the other data subject's right to privacy. NWL Collaboration of 8 CCGs should attempt, where practicable, to seek the consent of the third party to the release of their data. Where consent is obtained then the information can be released.

In some cases it may be extremely impractical to attempt to seek third party consent, and in these cases, or where consent has been sought but refused, NWL Collaboration of 8 CCGs may disclose the other parties' details where it is reasonable in all the circumstances to do so. For example it would be reasonable to make the disclosure where the other individual had already provided his or her data to the person making the request.

In other circumstances, the information may be so significant and of such importance to the applicant that he or she should be allowed access despite the fact that the other individual has not consented to the release of his or her information. In such a case even the release of confidential information may be justified. Reasons for failing to disclose information to the third party must be documented in the event of an assessment by the Information Commissioner's Office.

Where it is not reasonable to supply the third-party data, the information must be edited to remove any details that may lead to the identification of the third party. It is important to bear in mind that this editing must be applied to any information that might lead the data subject to infer the identity of the other party.

Given the sensitive and confidential information that NWL Collaboration of 8 CCGs hold, if there is any doubt about divulging third party information, legal advice must be sought before making a decision to release information.

6.4 Receiving an access request under the DPA

Applications for access to personal data by a data subject can be either verbal or in writing. For written application, please see the form in Appendix 2. It is not compulsory for a form to be completed by the data subject. The form is available to help in requesting for information. When a verbal request is made, this must be followed up with a letter or email to the requestor to clarify the request. The request for information must be sent to the subject access request mail box: nwlccgs.subjectaccessrequest@nhs.net

Written applications should be directed to the, DPO, NWL Collaboration of 8 CCGs, 15 Marylebone Road, NWL 5JD.

Applications must be signed and dated by the applicant.

Where an application is made on behalf of an individual, an authorisation letter duly signed and dated by the data subject must accompany the application.

The application must clearly identify the patient in question, and the records required, including the following details:

- Full name – including previous names
- Address – including previous address(es)
- NHS number (if available)
- Date of birth
- Dates of health/personnel records required
- Staff who are requesting records from Human Resources (HR) must complete the same application, which will be processed in the same manner and forwarded to HR

6.5 Provision of Information in response to a request

NWL Collaboration of 8 CCGs will provide to data subjects a copy of their information in an intelligible form and the use of jargon, abbreviations or codes contained within the information must be explained. If the information is terminologically difficult or of a technical nature, NWL Collaboration of 8 CCGs must offer to 'go through' the information with the data subject to explain the meanings. NWL Collaboration of 8 CCGs must take into account the provisions of the Disability Discrimination Act 1995 and the Equality Act 2010 and offer information in large print or Braille format for data subjects with visual difficulties. Where NWL Collaboration of 8 CCGs requested will allow data subjects to view their data.

Arrangements will be agreed with the data subject and relevant NWL Collaboration of 8 CCGs Managers to facilitate this within the timescales allowed by the Act (i.e. 30 working days). Where an access request has previously been complied with under the Act, NWL Collaboration of 8 CCGs does not have to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance (The Information Commissioner's office has defined a reasonable interval to be 12 months). Where NWL Collaboration of 8 CCGs does not hold the personal information requested, it will inform the applicant as quickly as possible.

6.6 Charges

NWL Collaboration of 8 CCGs will comply with the recommended charging fees within the boundaries as follows:

Viewing paper or Computer records	No Charge
Copying of only computer records	No Charge
Copying of paper records or a mix of computer and	No Charge
Viewing CCTV recorded image	No charge
Copying CCTV Recorded Image	No charge
Reports	No Charge
Excessive /Repetitive requests	Fee payable

6.7 Times of Disclosure

NWL Collaboration of 8 CCGs will respond to subject access request within the timescales outlined in the Data Protection Act 2018. When in exceptional cases of excessive request, NWL Collaboration of 8 CCGs has decided to charge a fee for a subject access request; it will inform the applicant that a fee is payable and the amount requested. NWL Collaboration of 8 CCGs is not required to provide the information requested until such time as the fee has been paid.

Responses to request for access must be made within one month of the date of receipt of the request and/or the fee payable. Failure to do so is a breach of the Act and could lead to a complaint to the Information Commissioner. Failure to comply with a request for subject access, without valid justification is treated as a serious matter and is investigated by the Information Commissioner. Such complaints are dealt with as a matter of priority and may often lead to a full scale investigation into an organisation's procedures and

practices. In exceptional circumstances, if it is not possible to comply with this period, the applicant should be informed. The CCG can extend the 30 days period for compliance with a GDPR data subject access request by a further two months where requests are complex or numerous.

6.8 Shared Records

There are situations where a subject access request involves a health record that is shared between healthcare organisations. The modernisation of health and social care will place a greater emphasis on shared records. In developing integrated health and social care service, NWL Collaboration of 8 CCGs will consider its arrangements for managing the requirements of the Data Protection Act 2018 and Subject Access requests with its partners as part of any service reconfiguration or development. The following principles will be followed where this is the case:

- Obligations under the Act are, in general placed on the holder of the record. If records are shared between two health or NHS bodies, they will be joint data controllers.
- Responsibility for ownership of the record rests with the Secretary of State for Health although essentially, where both organisations are joint data controllers for the shared record, both are controlling how they are used.
- In order to deal with Subject Access requests effectively, the organisation receiving the Subject Access request will take responsibility for processing the request and for obtaining consent or refusal for the release of parts of the record relating to the other organisation.
- Each organisation is obliged to deal with the access request and the authorisation to release the parts of the record in order to ensure the request is processed within the 30-day timescale.
- Each organisation takes responsibility for the access request and joint liability for their release where each organisation has authorised its release.
- If the organisation processing the access request ignores a decision made by the other organisation to exclude data from release and subsequently releases that element of the record, it will accept full liability.
- It is incumbent on each organisation to record the reasons why the release of a record is refused.
- If there is a refusal to disclose the record from the partner organisation, the organisation dealing with the access request should, in their response to the applicant explain the reason for the refusal and refer him/her to the other partner organisation directly if he/she wishes to contest the refusal.

Where the CCG is not the Data Controller for the information requested, the data subject should be directed to the Data controller to complete the request.

6.9 Freedom of Information Act 2000 requests

Responsibility for Freedom of Information Act (FOI) has been delegated to the North West London Collaboration of Clinical Commissioning Groups. All FOI requests should be forwarded to the FOI inbox ccgfoi@nw.london.nhs.uk. Please refer to the Freedom Of Information policy

6.10 Requests from public bodies and law enforcement agencies

The Data Protection Act outlines the circumstances in which some public bodies have statutory powers that enable them to request access to personal information. NWL Collaboration of 8 CCGs as a data controller will be extremely careful when releasing personal data to such parties and will, following receipt of a request, check that the organisation requesting the disclosure is acting within its powers by asking the applicant to quote the authority on which its power is based

NWL Collaboration of 8 CCGs will only accept the request if it is made in writing and it is able to verify the source of the request and any necessary test of prejudice carried out prior to releasing any personal data through its legal channels if necessary. Law enforcement agencies can request patient information on behalf of and where written consent has been obtained from the individual. If members of staff come across any such requests, they must inform the Head of Information Governance immediately.

The CCG regards all Personal Identifiable Information as confidential. (PID). PID should be treated with NHS code of confidentiality. Medical/Health records are considered as confidential data. Confidential information will not be disclosed without appropriate consent or other Legal basis as required by (Articles 6(1) for confidential Information and Articles 9(2) for "Special Categories of data", unless national policy requires otherwise, or where this is requested by legal authorities. Where Law enforcement requests confidential information, the request must be from a police rank of Inspector and above. The CCG reserves the right not to release confidential information without appropriate authorisation such as a power of attorney or court order

6.11 Incidents

Any incident involving a potential breach of the Data Protection Act 2018 or the Access to Health Records Act 1990 should be reported as an incident using the incident reporting form. Staff must complete a data incident/breach reporting form for all data incidents and information Governance breaches; this should be submitted to the generic NWL email address: nwlccgs.igenquiries@nhs.net and copy sent to the Information Governance lead and the DPO. A copy of the form can be found on the intranet under Information Governance. For IT incidents/breaches, staff must complete the NWLCCG IT Security Incident Reporting form; this should be submitted to the IT security team generic email address: nwlccgs.security@nhs.net. A copy of the form can be found on the intranet under Informatics/IT Security and Cyber security. (Please refer to the NWLCCG IT Security Incident Reporting Policy and Procedure)

Your line manager, the Data Protection Officer and the Caldicott Guardian should

also be informed of this and a decision will be taken whether it is necessary to report this as a Serious Incident and/or to the Information Commissioner.

6.12 Training

To ensure the successful implementation and maintenance of the Subject Access policy, staff must be appropriately informed and trained. Staff appraisal and personal development plans will identify individual needs and the CCG's training strategy and will link these into the wider expectations and requirements of the organisation with regard to the Knowledge and Skills Framework (KSF) competencies.

6.13 Review

The Data Protection Officer will review the policy annually.

7 Exemptions under the Data Protection Act 2018

What are exemptions?

In some circumstances, the DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, you may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain GDPR provisions.

This part of the Guide focuses on the exemptions in Schedules 2-4 of the DPA 2018. We give guidance on the exceptions built in to the GDPR in the parts of the Guide that relate to the relevant provisions.

The exemptions in the DPA 2018 can relieve you of some of your obligations for things such as:

- the right to be informed;
- the right of access;
- dealing with other individual rights;
- reporting personal data breaches; and
- Complying with the principles.

Some exemptions apply to only one of the above, but others can exempt you from several things. Refer to the safeguarding policy.

The data subject has a right to access the data the CCG holds on them. However, the CCG may restrict, wholly or partly the right of access, as long as the restriction has taken into consideration the data subject's fundamental rights and legitimate interest, a necessary and proportionate measure to –

1. Avoid obstructing an official or legal inquiry, investigation or procedure;
2. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

3. Protect public security;
4. Protect national security;
5. Protect the rights and freedom of others including trade secrets or intellectual property.

When we restrict the rights as above, we must inform the data subject that their rights have been restricted and the reasons for the restriction. We must also inform the data subject of their rights to make a request to the Information Commissioner's office, and their rights to lodge a complaint with the Commissioner and also their right to apply to a court under section 167 – compliance order of data protection act 2018.

Some things are not exemptions. This is simply because they are not covered by the GDPR. Here are some examples:

- **Domestic purposes** – personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity is outside the GDPR's scope. This means that if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the GDPR
- **Law Enforcement purposes** is outside the GDPR's scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the DPA 2018. See our [Guide to Law Enforcement Processing](#) for further information.
- **National security** – personal data processed for the purposes of safeguarding national security or defence is outside the GDPR's scope. However, it is covered by Part 2, Chapter 3 of the DPA 2018 (the 'applied GDPR'), which contains an exemption for national security and defence.

8 REFERENCES

- The Data Protection Act 2018
<http://www.legislation.gov.uk/ukpga/1998/29/introduction>
- Access to Health Records Act 1990
<http://www.legislation.gov.uk/ukpga/1990/23/introduction>
- Freedom of Information Act 2000
http://www.opsi.gov.uk/acts/acts2000/pdf/ukpga_20000036_en.pdf
- Best practice guidance for doctors and other health professionals on the provision of advice and treatment to young people under 16 on contraception, sexual and reproductive health – DOH 2004
http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4086960
- NHS Code of Confidentiality
- The General Data Protection Regulation ((EU) 2016/679) (GDPR)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253
- Department of Health Guidance for Access to Health Records Requests February 2010.
http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_112916

GLOSSARY

Information Commissioner – The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information.

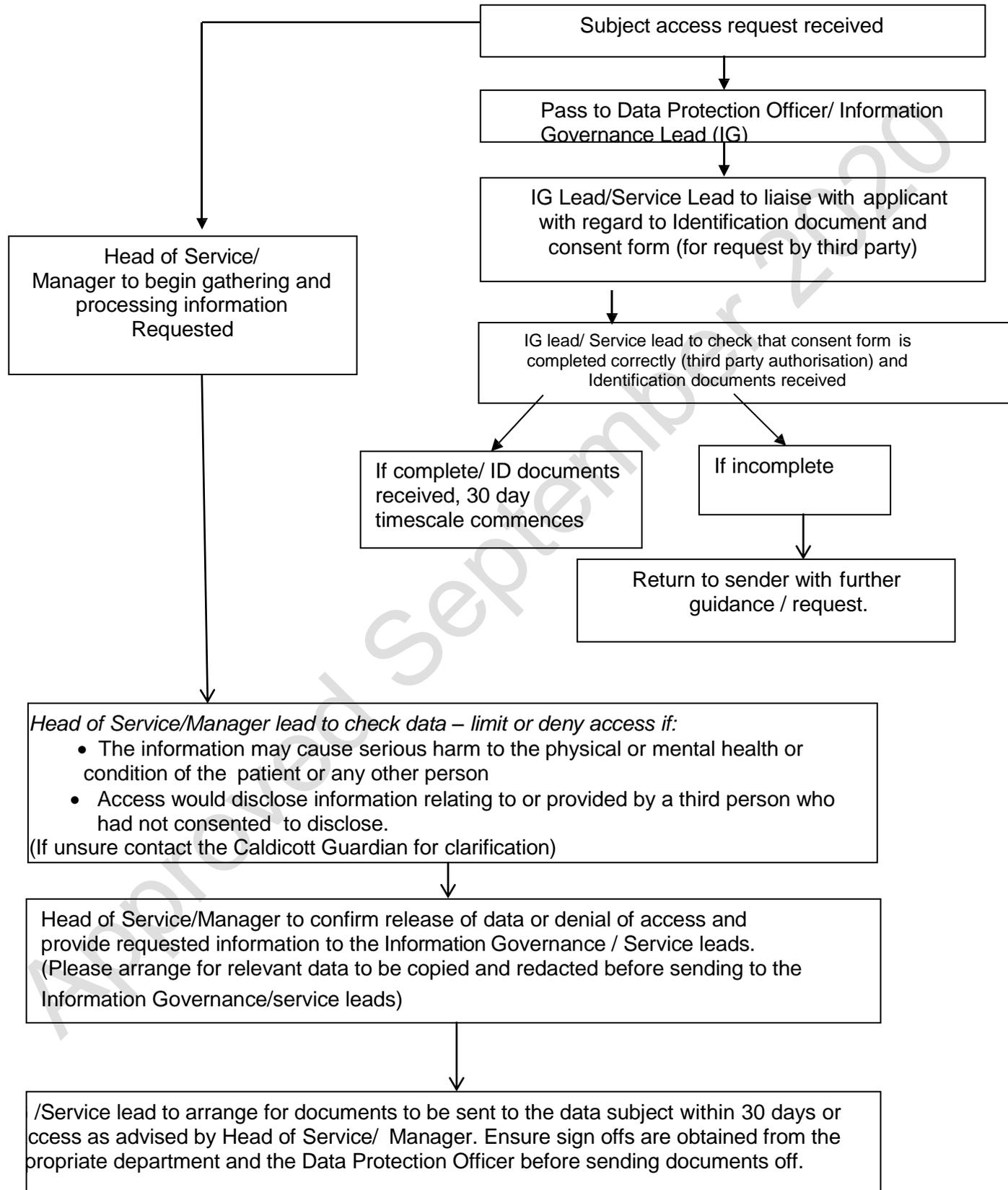
Data Controller – Whilst NWL Collaboration of 8 CCGs staffs are responsible for the collection of the data, the NWL Collaboration of 8 CCGs is responsible for determining the purposes for which and manner in which personal data is processed, and thereby NWL Collaboration of 8 CCGs as an organisation is the data controller.

Data Processor – The data processor in the CCG's case is all departments who process data except in the cases where NWL Collaboration of 8 CCGs uses third parties.

Data Subject – The Data Protection Act 2018 gives individuals who are the subject of personal data ("data subjects") a general right of access to the personal data which relates to them.

Access to Health Records At 1990 – The Act states that only two groups of people may access a deceased patient's health records: the patient's representative (executor or administrator of the estate) or anyone with a claim arising out of the patient's death.

Appendix 1 – Pathway for Responding to Subject Access Request



Appendix 2 – Subject Access Request Form

Subject Access Request Form (**Please note that a subject access request could be a verbal or written request**)

Subject Access Request – Data Protection Act 2018

This form is used to confirm the identity of the Staff / patient, the identity and authority of the applicant (where applicable) and to assist in locating information relating to the Staff / patient requested by the applicant. Please complete it and send it to the address at the end of the form. If you need any help please email:

nwlccgs.subjectaccessrequest@nhs.net

**PLEASE READ INFORMATION SECTION (Pages 6 – 8)
BEFORE COMPLETING THIS FORM**

Section 1 - Who is the data subject - Staff /Staff / patient?

Staff/Staff / patient's Surname	
Staff/Staff / patient's Forename(s)	
Date of Birth	
Hospital Number	
Address	
Country:	
Post Code:	

If the Staff / patient has lived at this address for less than 2 years please tell us their previous address	
Country:	
Post Code:	

Telephone number	

E-mail address

Section 2 - What are your personal details?

(a) Are you the staff/Staff / patient?

Yes

No

If you have answered “Yes”, go straight to Section 3 on page 3. Otherwise please provide the information below:

Your full name	
Address	
Country:	
Post Code:	
Telephone number	
E-mail address	

(b) If you are NOT the Staff / patient please tick the appropriate box below to state your relationship with them:

- I am the Staff / patient’s parent (with parental responsibility) and the Staff / patient is under 16 years old and: *(is incapable of understanding the request) (has consented to my making this request) *delete as appropriate
- I have been asked to act by the Staff / Staff / patient and attach the Staff / patient’s written authorisation
- I am the deceased Staff / patient’s Personal Representative and attach confirmation of this
- I have a claim arising from the Staff / patient’s death and wish to access information relevant to my claim and attach an explanation of the claim being considered
- I have been appointed as the Mental Capacity Advocate for this Staff / patient and wish to access copies of their records. I attach confirmation of my appointment
- Other? (please state):.....

.....

What written authority have you enclosed which supports your entitlement to the information you are requesting?	
---	--

Section 3 - Confirming your identity and address

(a) In order to confirm your identity, you will need to send us the original or a **certified copy*** of one of the documents listed below. Please tick the appropriate box to indicate which document you have enclosed:

- Full valid current passport issued by a member state of the EEA (European Economic Area)
- ID card issued by a member state of the EEA (European Economic Area)
- Full valid driving licence issued by a member state of the EEA (European Economic Area)
- Birth Certificate or Certificate of Registry of Birth or Adoption Certificate
- Travel documents issued by the Home Office
- Certificate of Naturalisation or Registration
- Home Office Standard Acknowledgement Letter

If your name is now different from that shown on the document you submit to confirm your identity, you must also supply documentary evidence to confirm the change of name. This must be the original or a **certified copy*** of a Marriage Certificate or Decree Absolute or Decree Nisi papers, Deed Poll or Statutory Declaration.

(b) You must also confirm your address by sending us the original or a **certified copy*** of one of the documents listed below. Please tick the appropriate box to indicate which document you have enclosed:

- Gas, electricity, water or telephone bill in your name for the last quarter
- Council tax demand in your name for the current financial year
- Bank, building society or credit card statement in your name for the last quarter
- Letter addressed to you from solicitor or social worker
- Pension Book or Jobseeker's Allowance Book

*A **certified copy** is one on which a person able to sign (e.g. Justice of the Peace, solicitor, medical doctor) has certified that it is a true copy of the original document.

(c) If you are applying on behalf of another person, you will need to show proof of **your** identity as well as theirs, plus proof that you have permission to act on their behalf. We will accept one of the following as proof that you have permission to act on their behalf. Please tick the appropriate box to indicate which document you have enclosed:

- A signed declaration by the Staff / patient
- A signed declaration by a health professional, police officer or MP confirming that the Staff / patient is unable to make the request themselves
- A document confirming that you are the parent or guardian of the Staff / patient

(if this is the case and the Staff / patient is a minor)

Section 4 – What information is requested

Please tick the appropriate box to indicate if you wish to access:

ALL records

or

Specific records regarding the treatment of (please state condition/illness and approximate date):

.....

.....

.....

.....

.....

.....

.....

<p>Please tick <u>ALL</u> relevant boxes to indicate which types of records you wish to access</p>	<p style="text-align: center;">Clinical Records (in Staff / patient & out Staff / patient)</p> <p><input type="checkbox"/> Accident & Emergency Records</p> <p><input type="checkbox"/> Medical records</p> <p><input type="checkbox"/> Staff / Personal records</p> <p><input type="checkbox"/> HR records</p>
<p>Please tick the appropriate box to indicate if you would you like copies of these records or just to view them</p>	<p style="text-align: center;">I would like to view the records</p> <p><input type="checkbox"/> I would like copies of the records</p>

Section 5 - Formal Declaration

In exercise of the right granted to me under the terms of the Data Protection Act 2018 (& EU GDPR), I request that you provide me with the information I have indicated overleaf. I confirm this is all of the information to which I am requesting access. I also confirm that I am either the Staff / patient, or am acting on their behalf. I am aware that it is an offence to unlawfully obtain such information, e.g. by impersonating the Staff /

patient. I certify that the information given in this form is true. I understand that it is necessary for the North West London (NWL) Collaboration of 8 Clinical Commissioning Groups (CCGs) to confirm my identity and it may be necessary to obtain more detailed information in order to confirm my identity and/or locate the correct information.

Signed	
Print name	
Date	

Please make sure you have:

- completed this form in full
- signed the declaration above
- enclosed the relevant proof of identity
- enclosed the relevant proof of address
- if applying on behalf of another person, their permission together with any authorities to act on their behalf

Send the completed form and enclosures to:

Email: nwlccgs.subjectaccessrequest@nhs.net

Postal Address:

Data Protection Officer
 1st Floor
 15, Marylebone Road
 London NWL 5JD

Note: We recommend that you send your form and documents by a secure method e.g. Recorded Delivery. North West London (NWL) Collaboration of 8 Clinical Commissioning Groups (CCGs) will return all original documents as soon as possible via recorded delivery. If you deliver your documents in person we will verify these at the time of your visit, retain copies of those documents and return them to you.

If you need any help please email: nwlccgs.subjectaccessrequest@nhs.net

Section 6 - Information

YOUR RIGHTS

Occasionally, it is important to see your records; especially if you are making a complaint, considering legal action or think that there may be inaccurate information in them. If you would like to see your records, you should ask the doctor or health professional to show them to you during a normal consultation and explain them to you.

If you do not want to do this, or the doctor or health professional is not able or willing to show you the records, you have the right to see your records under the Data Protection Act 2018. It applies to both NHS and private medical records and the records of employers who hold information on your health.

The Act gives right of access, but the record holder may withhold any information, which might cause serious harm to physical or mental health, or identify a third party. The record holder does not have to disclose the fact that information has been withheld.

Staff / patients have a right to have their personal health information kept confidential, and record holders are obliged to be satisfied that an applicant is the Staff / patient, or is otherwise entitled to access that Staff / patient's records. At the very least, we will need to confirm your identity, but we may also have to make further enquiries.

You can ask for corrections to the record, and you are entitled to a copy of the correction, or, if the record is not corrected, the record holder's note of the request and any discussion that has followed.

If you have been refused access to your record, or if you think you may not have received all the information, or if you are dissatisfied with the way your application has been dealt with; you should take the matter up in the first instance with PALS who can put you in contact with the designated officer for complaints, so that you can make a complaint under the NHS complaints procedure. If you are still dissatisfied you can complain to the Information Commissioner. For more information visit the relevant site at: <http://www.ico.gov.uk/>

RECORDS OF SOMEONE WHO HAS DIED

The statutory rights of access to these are contained within the Access to Health Records Act 1990 the provisions of which are very similar to those of the Data Protection Act 2018, and are summarised below:

- The Staff / patient's personal representative i.e. executor or administrator or someone applying on their behalf can apply for access to the health records. Legal documentation will be required to confirm appointment to this role.

Under the Access to Health Records Act 1990, a deceased person's representative can access information about the deceased. It should be noted that, a deceased person's next of kin is not necessarily the deceased person's representative.

If a will is made, then it is the executor of the will who is the lawful personal representative. If no will is made and the deceased died intestate, it is at this stage that the closest "next of kin" can apply, through a solicitor, for a **Letter of Administration** to handle the deceased's affairs.

- Any person who may have a claim arising out of the Staff / patient's death or someone applying on their behalf can apply for access to the health records. An explanation of the claim being considered will be required and no information which is not directly relevant to the claim may be released.

- Information may be withheld if the Staff / patient gave it in the past on the understanding that it would be kept confidential. Similarly, no results of examinations or investigations which the Staff / patient thought would be confidential at the time they were carried out can be disclosed. No information at all can be revealed if the Staff / patient requested non-disclosure.

CHILDREN

Children can apply to see their own records. A young person aged 13 or over or Gillick competent can access their medical records. A child under the age of 13 who is Gillick competent and who in the view of the appropriate health professional is capable of understanding what the application is about, can prevent a person with parental responsibility from having access to their records. In cases where, in the view of the health professionals, a child Staff / patient is not capable of understanding the nature of the application, the holder of the record is entitled to deny access to that child. Parents with parental responsibility (see below) can apply on behalf of a child under the age of 16, although normally the child will need to agree, if he himself/she herself has been declared Gillick competent. If the child is not able to understand the nature of the request, the record holder must be satisfied that it is in the interests of the child for the parents to see the records. Parents may not be allowed to see information which the child has given in confidence, such as about contraception or problems in the home.

Who has parental responsibility?

If the parents of a child are married to each other or if they have jointly adopted a child, then they both have parental responsibility. This is not automatically the case for unmarried parents. According to current law, a mother always has parental responsibility for her child. A father, however, has this responsibility only if he is married to the mother or has acquired legal responsibility for his child through one of these three routes:

- (after 1 December 2003) by jointly registering the birth of the child with the mother
- by a parental responsibility agreement with the mother
- by a parental responsibility order, made by a court

Living with the mother, even for a long time, does not give a father parental responsibility and if the parents are not married, parental responsibility does not always pass to the natural father if the mother dies. A father can apply to the court to gain parental responsibility.

Source: http://www.direct.gov.uk/en/Parents/ParentsRights/DG_4002954

FEES

You will **no longer** be *charged for copies of the notes that are released to you (**please do not send any money or cheques with your application form**).

To allow Staff / patients to **view** their health records (where no copy is required) there are NO costs:

- Where the request is for either manual files or computer files or a mixture of manual files and computer files

To provide **copies** of Staff / patient health records:

- Where the request is for files held solely on a computer the CCG will no longer charge you

- Additionally, fees are not applicable to individuals in receipt of certain benefits such as Jobseeker's Allowance, nor will the NWL CCGs apply fees to requests from other NHS trusts, the police, the Coroners' Office or the courts.

*charges will only be applicable for excessive/repetitive requests.

Approved September 2020

Appendix 3 - Essential ID Documents

The applicant should present either **two forms of photo ID or one proof of address OR one form of photo ID and two proofs of address.**

Acceptable photographic personal identification

- Full, signed UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passport
- UK Biometric Residence Permit (BRP) card
- UK full or provisional photo card driving licence
- EU/other nationalities photo card driving licence (valid up to 12 months up to the date of when the individual entered the UK and providing that the person checking is confident that non-UK photo card driving licences are bona fide).
- HM Armed Forces Identity card (UK)
- Identity cards carrying the PASS (Proof of Age Standards Scheme) accreditation logo (UK and Channel Islands). Organisational identity cards are not acceptable as they do not contain watermarks, holograms or other security markings.

Acceptable confirmation of address documents

- Utility bill (**gas, water, electricity or landline telephone ONLY**), or a letter from a utility supplier confirming the arrangement to pay for the services at a fixed address on pre- payment terms. More than one utility bill may be accepted, if these are from **two different suppliers**. Utility bills in joint names are also acceptable (UK)*
- Local authority tax statement. For example, a council tax statement (UK and Channel Islands)**
- UK full or provisional photo card driving licence if not already presented as a form of personal photographic identity.
- HM Revenue & Customs tax notification (HMRC) tax notification such as an assessment, statement of account, notice of coding** **NOT a P45 or P60**
- A financial statement such as **bank, building society, or credit card statement*** (UK and EEA). Statements issued outside of the EEA must not be accepted. More than one financial statement may be accepted if they are from **two different organisations**.
- Credit union statement (UK)*
- Mortgage statement from a recognised lender** (UK and EEA). Statements issued outside of the EEA must not be accepted.
- Local council rent card or tenancy agreement*
- Evidence of entitlement to Department for Work and Pensions benefits, such as child allowance, pension etc. (UK)**
- Confirmation from an electoral register that a person of that name lives at the claimed address**

* All documents must be dated within the last 3 months

** All documents must be dated within the last 12 months

Appendix 4 – Equality Impact Assessment

Equality Impact Assessment Tool (Equality Analysis)

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/ No	Comments
1	Does the policy/guidance disadvantage one group or more than another on the basis of:		
	<ul style="list-style-type: none"> ▪ Race (including colour, culture, ethnicity, nationality or national origin and the travelling community) 	N	
	<ul style="list-style-type: none"> • Religion or Belief 	N	
	<ul style="list-style-type: none"> • Sex (e.g. male or female) 	N	
	<ul style="list-style-type: none"> • Marriage or Civil Partnership 	N	
	<ul style="list-style-type: none"> • Sexual Orientation (Lesbian, Gay, Bisexual, Heterosexual) 	N	
	<ul style="list-style-type: none"> ▪ Gender reassignment (e.g. someone who 'is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.') 	N	
	<ul style="list-style-type: none"> • Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.) 	N	
	<ul style="list-style-type: none"> • Pregnancy and Maternity 	N	
	<ul style="list-style-type: none"> • Age (children, young adolescent, older people etc.) 	N	
2	Is the policy/guidance/strategy more favourably towards one group on the basis of:		
	<ul style="list-style-type: none"> • Race 	N	
	<ul style="list-style-type: none"> • Religion or Belief 	N	
	<ul style="list-style-type: none"> • Sex 	N	
	<ul style="list-style-type: none"> • Marriage or Civil Partnership 	N	
	<ul style="list-style-type: none"> • Sexual Orientation 	N	
	<ul style="list-style-type: none"> • Gender reassignment 	N	

	<ul style="list-style-type: none"> Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.) 	N	
	<ul style="list-style-type: none"> Pregnancy and Maternity 	N	
	<ul style="list-style-type: none"> Age (e.g. children, young adolescent, older people etc.) 	N	
3	If you have identified potential discrimination in the policy/guidance are there any valid, legal and/or justifiable exceptions? Please list any exceptions.	N/A	
4	Is the policy/guidance likely to have a negative/adverse impact on any of the above group(s)?	N/A	
5	If so, how would you address the impact? Please explain.	N/A	

If you have identified a potential discriminatory impact in this document, please refer to the author(s) of the policy/guidance, together with any suggestions required to address the impact.