Subject Access Request Policy (CWHHE/GOV/007)

Understanding of, and compliance with, this policy is a contractual obligation of all employees (including contractors, interims, volunteers, office holders) of the CCGs. Failure to do so may lead to disciplinary action up to and including dismissal.

Document Reference Information

Version:	1.0		
Date completed:	October 2017		
Responsible Director:	Director of Compliance	**Author:**	Riordan Hill
Approved by/ date:	tbc		
Review date:	October 2018		
Amended:			

Version Control Record

Date	Version	Action	Amendments
October 2017	1.0	First version to be approved by Governing Body in November 2017	

Other relevant documents to this policy:
Safeguarding Children Policy
Policy for obtaining legal advice
Confidentiality and Data Protection Policy
Information Governance Policy
Incident Reporting and Management Policy

CONTENTS

1. Introduction

1.1 CWHHE Collaboration of CCGs (referred to as 'the CCGs' throughout are required to ensure that they have a policy and procedure in place to respond to Subject Access Requests under the Data Protection Act 1998.

1.2 This policy deals with the rights of data subjects under the Data Protection Act. 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 written 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 CCGs. This applies to anyone about whom the CCGs hold information – including staff, ex-staff, residents, service users, independent contractor suppliers, and contractors. This policy will provide a framework for the CCGs to ensure compliance with the Data Protection Act 1998.

3. The Data Protection Act 1998

3.1 The Data Protection Act 1998 (DPA) 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 eight "data protection principle" set out in Schedule 1, Part 1 of the Act.

3.2 The Information Commissioner's Office (ICO) is the UK's independent public body that is responsible for governing Data Protection compliance: www.ico.org.uk/

3.3 The DPA 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 sections 7, 8 and 9 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.

3.7 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 CCGs will ask for a copy of the Grant of Probate or Letters of Administration. The CCGs understand that these documents are not always available so will 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 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 CCG's Governing Body

The Governing Body has a duty to ensure that the requirements of the Data Protection Act 1998 are upheld.

5.2 **Caldicott Guardian**

The Caldicott Guardian of the CCGs (Director of Quality and Safety) is responsible for ensuring that the CCGs are compliant with the confidentiality requirements of the Data Protection Act.

5.3 **Data Protection Officer**

In order to ensure that the CCGs are able to meet the requirements of the Data Protection Act 1998 and Subject Access Requests requirements consistently, the CCGs have appointed a single person to act as Data Protection Officer.

The Data Protection Officer is responsible for:

- over-seeing the systems and procedures that support the implementation of this policy;
- **ensuring** consent is obtained from the individual for the release of their records/data, in accordance with the requirements of the Data Protection Act 1998 and NWL CCGs guidelines and procedures for Subject Access Requests under the Data Protection Act 1998;
- providing advice to nominated Directorate/departmental Leads and/or Heads of Service/Senior Managers on exemptions and exclusions under the Data Protection Act;
- liaising with other organisations to process the access request in the event of shared records/data; and
- co-ordinating the release of the information and ensure that sufficient identification is given by the applicant.

5.4 Service Leads will be responsible for:

- ensuring that 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 that the record / data is reviewed by an appropriate professional and the identification of exemptions, and third party information in accordance with the Data Protection Act;
- approval for data release is undertaken by a senior and appropriate professional and this approval exercise undertaken as a priority; and
- ensuring their staff are aware of this policy

5.5 All individuals undertaking official CCG on behalf of the CCG are required to read, understand and adhere to this policy.

6. IMPLEMENTATION

6.1 Subject Access Requests – the rights of individuals

The DPA 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 under Section 7.

Section 7 of 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 Commissioners 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 the 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 Lasting (or, pre-2007, 'Enduring') Power of Attorney). For further guidance, see the Mental Capacity Act.

A young person over 16, but under 18, or a child under 16 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, the 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. The 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 the CCGs' 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, the 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. 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, 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 CWHHE CCGs sometimes 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 must be made in writing using Appendix 2.

Applications should be directed to the Governance & Compliance Team, 15 Marylebone Road, London, NW1 5JD

Applications must be signed and dated by the applicant and proof of identity of the applicant (and her or his representative) provided. Upon receipt of such, and any payments required (see 6.6), the CCG has 40 days to fulfil the request.

Where an application is made on behalf of an individual, an authorisation letter must accompany the application. The letter should state "I hereby authorise the CCG to release any information they may hold relating to me to [enter the name of the person acting on the subject's behalf] to whom I have given my consent to act on my behalf." The letter must be dated with a signature.

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; and
- Dates of / period from which 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

The 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, the CCGs must offer to 'go through' the information with the data subject to explain the meanings. The 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.

Arrangements will be agreed with the data subject and the relevant CCG Managers to ensure the request is facilitated within the timescales required by the Act. Where an access request has previously been complied with under the Act, the CCGs do not have to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance (defined by the ICO

as 12 months). Where the CCG does not hold the personal information requested, it will inform the applicant as quickly as possible.

6.6 Charges

The 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 paper records	£10 + 30p per copy (Maximum charge £50)
Viewing CCTV recorded image	No charge
Copying CCTV Recorded Image	£10 (Maximum charge)
Reports	Charged at department's discretion

6.7 Times of Disclosure

The CCGs will respond to subject access request within the timescales outlined in the Data Protection Act 1998. Where the CCGs have decided to charge a fee for a subject access request, it will inform the applicant that a fee is payable and the amount requested. The CCGs are 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 40 days 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.

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, the CCGs will consider their arrangements for managing the requirements of the Data Protection Act 1998 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 body, Trust etc;
- 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 40-day timescale;
- each organisation takes responsibility for the access request and joint liability for their release where each has authorised its release;
- if the organisation processing the access request ignores a decision made by the other 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; and
- 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.

6.9 Freedom of Information Act 2000 requests

All FOI requests should be forwarded to the FOI inbox ccgfoi@nw.london.nhs.uk.

6.10 Requests from public bodies and law enforcement agencies

Section 29 of the Data Protection Act outlines the circumstances in which some public bodies have statutory powers that enable them to request access to personal information. 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.

The 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 governance and compliance directorate.

6.11 Incidents

Any incident involving a potential breach of the Data Protection Act 1998 or the Access to Health Records Act 1990 should be reported as an incident to the

governance team. Your line manager 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 under the Serious Incident Reporting and Management Policy 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 will link these into the wider expectations and requirements of the organisation with regard to KSF competencies.

6.13 Review

This policy will be reviewed the annually, or as any additional requirements emerge.

7 REFERENCES

- The Data Protection Act 1998
  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
  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

8. 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 the CCGs staffs are responsible for the collection of the data, the CCGs are responsible for determining the purposes for which and manner

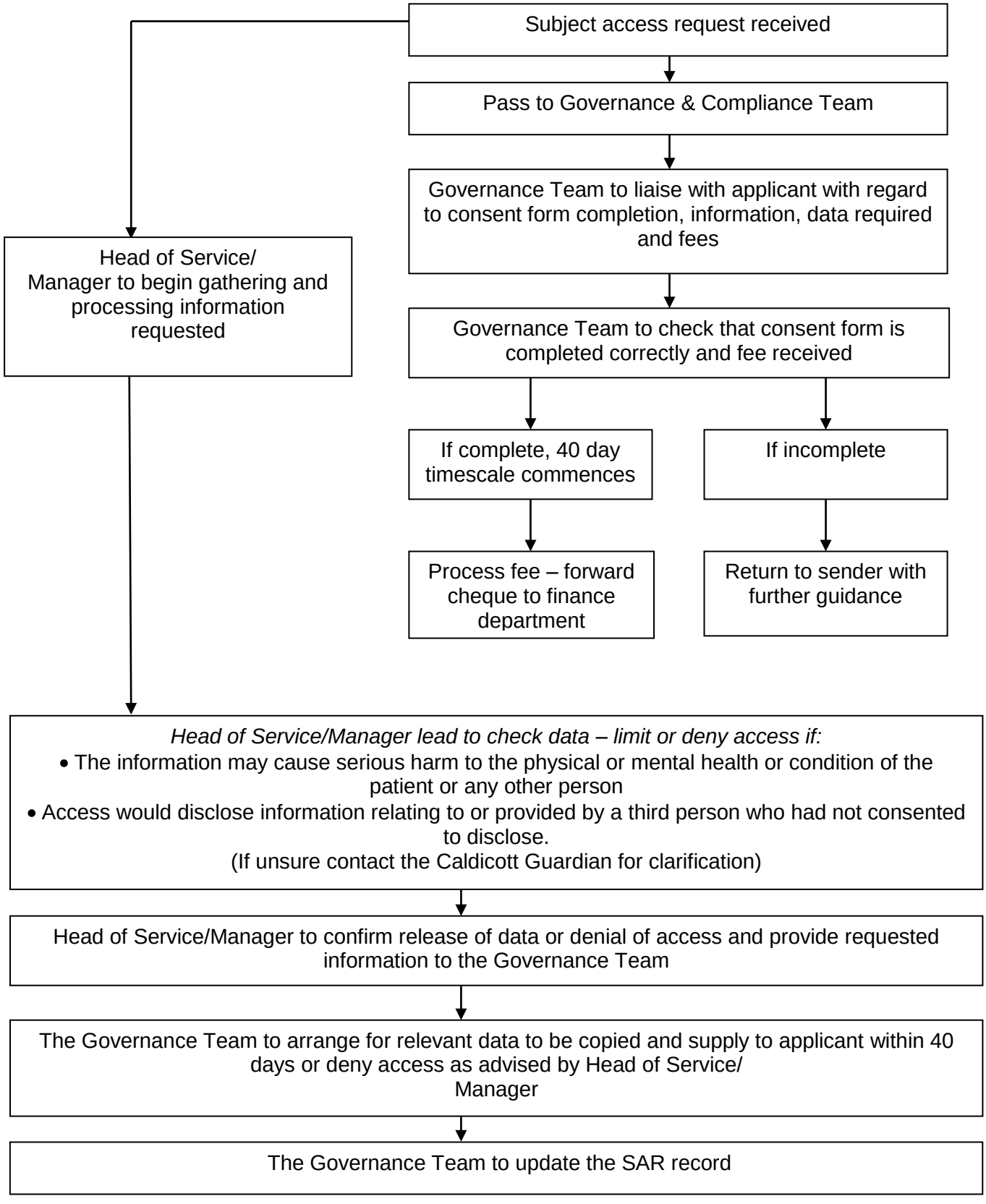
in which personal data is processed, and thereby BHH CCGs as an organisation is the data controller.

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

Data Subject – The Data Protection Act 1998 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

	Personal information collected from you on this form is required to enable your request to be appropriately processed. This personal information will only be used in connection with the processing of this Subject Access Request.

1. Details of the person requesting the Information			
Surname:	……..	First Names(s):	……..
Maiden Name:	……..	Date of Birth:	……..
Telephone Number:	……..	NHS Number:	……..
Address & Postcode	…… …… …… …… ……		

2. Are you the Data Subject? (tick box that applies)	
I **AM** the Data Subject and enclose evidence of my identity e.g. photocopy of driving licence, birth certificate, passport, marriage certificate.	☐
I am **NOT** the Data Subject, but am acting on their behalf as their personal representative. I have written authority, which I enclose and evidence of their identity e.g. photocopy of driving licence, birth certificate, marriage certificate, passport.	☐
I am **NOT** the Data Subject, but I am acting on their behalf as their parent or legal guardian and enclose evidence of their identity and my identity e.g. photocopy of birth certificate, passport. I also enclose written consent from the subject to access their information or other evidence that I am entitled to access their information.	☐

3. Details of the Data Subject (if different to 1.)			
Surname:	……..	First Names(s):	……..
Maiden Name:	……..	Date of Birth:	……..
Telephone Number:	……..	NHS Number:	……..

Address & Postcode	…… …… …… …… ……

4. Describe the specific information you are requesting: please provide as much detail as possible, such as relevant dates, references, treatments etc. Include which CCGs the request is relevant to.

5. Declaration			
I declare that the information given by me is, to the best of my knowledge correct and that I am entitled to apply for access to the information referred to above, under the terms of the Data Protection Act 1998.			
Signature:		Date of Request	

6. The following charges will apply until reviewed:- (Please make cheques payable to NHS Central London CCG)	
Viewing paper or Computer records	No Charge
Copying of only computer records	No Charge
Copying of paper records or a mix of computer and paper records	£10 + 30p per copy (Maximum charge £50)
Viewing CCTV recorded image	No charge
Copying CCTV Recorded Image	£10 (Maximum charge)
Reports	Charged at department's discretion

PLEASE RETURN TO:
Governance Team
NWL CCGs
15 Marylebone Road
NW1 5JD

For use by Governance & Compliance Team Only

Date Request Received		Amount Paid	
Date Form sent to applicant		Method of Payment	
Date Form Returned		Date sent to System Administrators/Service Lead	
Certification Checked		Date Data checked	
		Date completed and sent	

A written response to your application will be made within 40 days.

Appendix 3 – Equality Impact Assessment

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

DOCUMENT AUTHOR: Corporate Governance Manager, CWHHE CCGs	DIRECTORATE: Governance
NAME OF DOCUMENT/POLICY/STRATEGY/PROCEDURE Subject Access Request Policy	NEW EXISTING ASSOCIATED POLICIES, STRATEGIES OR PROCEDURES
DATE: 30th October 2017	

Aim/Status

[a] What is the aim/purpose of the policy/strategy/procedure? To provide a clear policy, procedure and protocols for staff and patients.
[b] Who is intended to benefit from this policy/strategy/procedure and in what way? Staff and patients in CWHHE CCGs leading to improved communication and an enhanced service.
[c] How have they been involved in the development of this policy/strategy/procedure? Policy has been discussed with Information Governance leads.
[d] How does it fit into the broader corporate aims? The policy supports delivery of the corporate objectives of the CCGs, particularly the sixth objective, ensuring we have the capacity and capability to deliver.
[e] What outcomes are intended from this policy/strategy/procedure? Improved response to individuals who request to access their personal data held by the CCGs.
[f] What resource implications are linked to this policy/strategy/procedure? None – we already respond, this policy describes the process. we do need to consider where the role of Data Protection Officer should best sit. It currently sits with the Deputy Senior Information Risk Owner (Director of Compliance)

Impacts

[a] what is the likely impact [whether intended or unintended, positive or negative] of the initiative on individual users or on the public at large? This will give staff and requestors of data a written policy and procedure to follow thus supporting people to comply with the Data Protection Act.		
[b] Is there likely to be differential impact on any group? If yes, please state if this impact may be adverse and give further details [e.g. which specific groups are affected, in what way, and why you believe this to be the case] No		
[i] Grounds of race, ethnicity, colour, nationality or national origin	Please tick box no	Please tick box Adverse? ☐ Please give further details

[ii] Grounds of sex or marital Status Women and Men	no	Adverse?☐ Please give further details
[iii] Grounds of gender: Transgender or Transsexual People	no	Adverse? ☐ Please give further details
[iv] Grounds of religion or belief: Religious /faith or other Groups with a recognised belief system	no	Adverse? ☐ Please give further details
[v] Grounds of disability	no	Adverse?☐ Please give further details
[vi] Grounds of age: Older people, children and Young people	no	Adverse?☐ Please give further details
[vii] Grounds of sexual orientation: Lesbian, gay, bisexual	no	Adverse?☐ Please give further details
[viii] Grounds of carers: Older relatives, children	no	Adverse? ☐ Please give further details
[ix] Grounds of human rights	no	Adverse?☐ Please give further details

Is the policy directly discriminatory? No	Is the policy indirectly discriminatory? No If you said yes, is this objectively justifiable or proportionate in meeting a legitimate aim yes ☐ no ☐	Is the policy intended to increase equality of opportunity by permitting positive action or action to redress disadvantage No
If the policy is unlawfully discriminatory it must go to a full impact assessment (please Contact the Equality, Diversity & Human Rights Advisor – Human Resources Directorate)		