

## ACCESS TO HEALTH RECORDS BY PATIENTS OR THEIR AUTHORISED REPRESENTATIVE POLICY

Version:	3.0
Approved by:	Data Security and Protection Group
Approval date:	23 <sup>rd</sup> February 2018
Ratified by:	Audit Committee
Date ratified:	
Name & job title of author	Rob Lavender, RA Manager
Name of responsible committee	DSPG
This document covers:	The management of requests to view health records (Subject Access Requests)
Original Date issued:	17 October 2013
Review date:	23 <sup>rd</sup> February 2019

Version	Date	Author(s)	Status	Comment Changes
0.1	04/10/13	Rob Lavender	Draft	For approval
1.0	17/10/13	Rob Lavender	Approved	Ratified
1.1	22/12/2016	Ernest Norman-Williams	Review	Annual Review
1.2	20/10/2017	RM	Review	Annual Review
2.0	23/02/2018	SL	Approved	Approved by DSPG
2.1	30/08/2018	Rebecca Bada	Approved	Updated to comply with GDPR
3.0	24/09/2018	RM	Approved	Ratified

## Contents

<b>1. Introduction</b>	<b>3</b>
<b>2. The Data Protection Act (2018)</b>	<b>3</b>
<b>3. Caldicott Guardian</b>	<b>3</b>
<b>4. Other Guidance</b>	<b>4</b>
<b>5. Definition of a Health Record</b>	<b>4</b>
<b>6. Duty of Confidence</b>	<b>4</b>
<b>7. Access by Patients or Their Representative</b>	<b>5</b>
<b>8. Subject Access Request forms</b>	<b>6</b>
<b>9. Access to Children’s Health Records</b>	<b>6</b>
<b>10. Requests From Outside the UK</b>	<b>7</b>
<b>11. Access to Health Records of a Deceased Person</b>	<b>7</b>
<b>12. Fees</b>	<b>7</b>
<b>13. Response Targets</b>	<b>8</b>
<b>14. When a request could be refused</b>	<b>8</b>
<b>15. Procedures</b>	<b>9</b>
<b>16. Confirming Identity</b>	<b>9</b>
<b>17. Providing or Denying Access</b>	<b>9</b>
<b>18. Correcting a Record</b>	<b>10</b>
<b>19. The Information Commissioner’s Office (ICO)</b>	<b>11</b>
<b>Appendix A</b>	<b>12</b>
<b>Appendix B</b>	<b>13</b>
<b>Appendix C</b>	<b>14</b>
<b>Appendix D</b>	<b>15</b>
<b>Appendix E</b>	<b>16</b>
<b>Appendix F</b>	<b>18</b>
<b>Appendix G</b>	<b>20</b>

## 1. Introduction

This policy gives direction to staff at Barking and Dagenham, Havering and Redbridge CCGs (BHR CCGs) about the provision of access (known as Subject Access) to health records for patients and their representatives.

This policy applies to all health records held by BHR CCGs (the Organisation) and also applies to entries made by health professionals in records for integrated services.

In line with Government policy the Organisation will offer a copy of any correspondence relating to the health care of a patient, provided by the Organisation, to the patient. This offer is subject to conditions under the Data Protection Act (DPA) (2018).

## 2. The Data Protection Act (2018)

The Data Protection Act (2018) gives every living person, or their authorised representative, the right to apply for access to their health records, irrespective of when they were compiled. See Appendix E for request template.

This Act became effective from 25<sup>th</sup> May 2018. It superseded the Data Protection Act (1998) and the Access to Health Records Act (1990). The exception to this is access to the health records of deceased persons, which are still governed by the Access to Health Records Act 1990, which is referred to in Section 11 of this policy.

The DPA (2018) outline 6 key principles relating to the approach of processing personal data, following as:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)

## 3. Caldicott Guardian

The Organisation has a Caldicott Guardian who is responsible for health records and whose role is to ensure that the Organisations records strategies are in line with national requirements. These requirements reflect the 6 principles set out in the Caldicott Report 1997 to govern the access to and use of confidential information:

- The purpose of using confidential information must be justified.
- Confidential information must only be used when absolutely necessary.
- The minimum necessary to achieve the purpose should be used.
- Access to confidential information must be on a strict need-to-know basis.

- Everyone accessing confidential information must understand his or her responsibilities.
- Everyone accessing confidential information must comply with the law.
- 

#### **4. Other Guidance**

This policy has been written in line with the Department of Health Guidance for Access to Health Records requests under the Data Protection Act (2018).

This policy should be read in conjunction with the following Organisations policies:

- Information Security and Access Control Policy
- Data Protection and Confidentiality Policy
- Information Governance Policy
- Information Lifecycle Policy

If a request for a report about a patient to a third party (e.g. solicitor, insurance company etc.) is received staff should contact the Caldicott Guardian for further advice.

Further guidance can be obtained from the Information Commissioner at the address quoted in paragraph 19 of this policy.

#### **5. Definition of a Health Record**

A health record is defined 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. It may be recorded in computerised form or manual form or a mixture of both. The record may include hand written clinical notes, letters, laboratory reports, x-rays and imaging reports, print-outs of monitoring equipment, photographs, videos, tape recordings of conversations and computer held health records.

Current legislation also means that private health records are treated as all other health records.

Health records have the following functions:

- Supporting patient care
- Assisting in the day to day management of patients
- Assisting evidence based practice
- Assisting managerial decision making of importance to the NHS as a whole
- Assisting in audit
- Assisting in the advancement of clinical effectiveness

#### **6. Duty of Confidence**

All those working for or with the Organisation, who record, handle, store or otherwise have access to health records have a personal, common-law duty of confidence. All of

the Organisations employees have a duty to maintain professional ethical standards of confidentiality.

Any personal health information, given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else, without the consent of the patient or provider of the information. However, this is not an absolute duty and can be subject to an overriding public interest. For example, where failure to disclose would place a vulnerable child or adult at risk of harm, disclosure has to be considered. Similarly, where a person carrying a life-threatening transmissible infection is believed to be acting irresponsibly, disclosure in the course of protecting the health of other people has to be considered. Orders of a court to disclose information should be complied with.

In accordance to the first principle of the DPA (2018), a breach of a duty of confidence is deemed as unlawful. The DPA (2018) grants individual the right to erase that data or restrict the processing of the data if, personal data has been processed unlawfully.

## **7. Access by Patients or Their Representative**

A patient, or their representative with their consent, has the right to apply for access to their health records.

The DPA (2018) does not state specifically how a valid request can be made, therefore an individual has the option to make a subject request to any part of the organisation either verbally or in writing (also via social media) and does not have to be to a specific person or contact point.

As long as it has been made clear that an individual is asking for their own personal data, they are not obliged to use the phrase of 'subject access request' or Article 15 of the DPA (2018).

If a request is received from a patient's representative the patient must authorise the release of their record. The patient's representative may be a relative, friend, legal representative or any other person that the patient consents to have access to their record.

If a patient is unable to authorise the release of their record due to a lack of mental capacity then a person who has been legally appointed to act on the patient's behalf has the right to apply for access to the health record of the patient. Such a person should be asked to produce evidence that they hold a lasting power of attorney or Deputyship Order under the Court of Protection which allows the person to make decisions regarding finances, property and/or welfare. A legal power of attorney must be registered with the Office of the Public Guardian.

An Independent Mental Capacity Advocate (IMCA) is a statutory form of advocacy that provides safeguards for people who lack capacity to make decisions about:

- Serious medical treatment or

- Moving into, or between, care settings (including hospital).

An IMCA is entitled under the Mental Capacity Act 2006 to ask for access to the person's medical and health records, and to take copies from these.

## **8. Subject Access Request forms**

DPA (2018) states that organisations should 'provide means for requests to be made electronically, especially where personal data are processed by electronic means'. See Appendix C, D and E for the template.

Electronic requests should be responded to in a commonly used electronic format unless the individual requests otherwise.

Despite creating an electronic subject access request form, it must be made clear to individuals that it is permissible to submit their request by a letter, a standard email or verbally.

The DPA (2018) also includes a best practice recommendation that, where applicable, organisations should also provide remote access to a secure self-service system which would provide the individual with direct access to his or hers information (Recital 63).

## **9. Access to Children's Health Records**

Under the DPA (2018), children age 13 and over are competent enough to provide their own consent. Therefore, the organisation will need to verify that the individual giving their own consent meets the age requirement.

In relation to children under the age of 13, efforts must be demonstrated (using available technology) to verify that the person given consent holds parental responsibility for the child.

Parental responsibility for a child is defined in the Children's Act 1998 as 'all the rights, duties and powers, responsibilities and authority which by law a parent of a child has in relation to the child and his property'. Current law states that a mother always has parental responsibility for her child. A father has the responsibility only if he was married to the mother at the time of the child's birth or has acquired legal responsibility. Parental responsibility can also be acquired by the local authorities if the child is under a care order.

Parental responsibility would include:

- Safeguarding and promoting a child's health, development and welfare
- Financially supporting the child
- Maintaining direct and regular contact with the child

Responses should be given directly to the child if the organisation is confident that the child is mature enough to understand their rights. Information provided to the child must be the same information given to adults. It is good practise to explain the risk inherent processing, and how we intend to safeguard against them, in a child friendly way, so

that children (and their parents) understand the implications of sharing their personal data.

The child needs to be able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

When dealing with borderline cases, the organisation should take into account, among other things:

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

## **10. Requests From Outside the UK**

Requests from patients living outside of the UK should be treated the same as requests from within the UK.

## **11. Access to Health Records of a Deceased Person**

Access to the health record of a deceased person is governed by the Access to Health Records Act 1990. Under this legislation where a patient has died, their personal representative (this may be the next of kin), executor, administrator or anyone having claim resulting from the death has the right to apply for access to the deceased's health record – see Appendix F.

Information about a deceased person does not constitute personal data so therefore is not subject to the DPA (2018).

## **12. Fees**

Previously, under the Data Protection Act 1998 (Fees and Miscellaneous Provisions) regulations 2001, a patient can be charged to view their health records or to be provided with a copy of them.

However, the DPA (2018) now states that organisations cannot charge a fee to comply with a subject access request. Although, a reasonable fee (based upon administrative cost) can be applied where the request is manifestly unfounded or excessive.

### **13. Response Targets**

The DPA (2018) requires organisations to act on the subject request without undue delay and at the latest within 28 days of receipt.

The time limit should be calculated from the day after the subject access request is received (whether the day after is a working day or not) until 28 days later.

The grounds on which the time can be extended for a response is when the request is complex or a number of request have been made from the individual.

Response time is permitted to extend by a further two month, however the organisation must inform the individual within one month of receiving their request and explain why the extension is necessary.

A log recording all access requests shall be held centrally by the Caldicott Guardian to monitor requests.

### **14. When a request could be refused**

The organisation can refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature

In this case you can:

- Request a “reasonable fee” to deal with the request; or
- Refuse to deal with the request.

In circumstances other than those listed above, you must justify your decision.

If the decision is made to refuse a request, the individual must be informed without delay and within 28 days of receipt of the request.

When informing the individual, the following must be mentioned:

- 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.

This information must also be provided when you request a reasonable fee or need additional information to identify the individual.

## 15. Procedures

Requests for access can be made verbally and in writing (including via social media). Forms included in the appendices should be used, however Subject Access Requests will still be accepted without a form.

If a patient's representative e.g. solicitor, is applying for access, ensure that it includes the written consent of the patient. If no consent is given, the request should be returned to the applicant for written consent to be obtained.

Additional information (only to confirm identity) may be requested if doubts are raised about the identity of the person making a request. Dealing with the request may be put on hold until additional information is provided.

## 16. Confirming Identity

Once patient consent is obtained due consideration must be given to the information submitted to confirm the identity of the patient e.g. full and previous name, date of birth, current and previous address, NHS number. Unless the health professional is satisfied as to the identity of the patient or applicant a request for evidence of identity should be made. This could include passport, driving licence, paid utility bill or any document that might reasonably be only in their possession.

Check with the applicant to confirm what material is required before processing the request. This could decrease the financial cost of copying for the applicant and eliminate unnecessary work for the staff. The applicant does not have to give a reason for requesting access and therefore may not wish to identify the part of the record required, in which case the entire record should be copied, or made available for viewing, and the applicant advised of any charge.

## 17. Providing or Denying Access

Once all the necessary information for an access request and fee, where relevant, is received, the request should be complied with promptly. If an access request cannot be dealt with promptly the applicant should be informed.

A log should be kept of the request (see appendix A). The log is the responsibility of the nominated representative of the Caldicott Guardian. A copy of the log entry should be sent to the Caldicott Guardian.

Once the log is completed an appropriate health professional should be consulted. This should be the individual who is, or was, responsible for the clinical care of the patient during the period to which the application refers. If there is more than one health professional then the most senior available health professional concerned should be approached to advise on whether to release other health professional's notes about that patient. Only the Caldicott Guardian or the Deputy Caldicott Guardian can approve the final release of records.

Before the patient's health record is released the health professional should ensure that they have checked the record and considered if allowing access:

A. Could result in serious harm to the physical or mental health condition of the patient, or of any other person.

Or

B. Would disclose information relating to, or provided by a third person (not a health professional), who had not consented to that disclosure. This should always be considered if the record applies to care given by an integrated service e.g. service provided by health professionals and social services together.

If either of these applies then the health professional may deny or limit access to the record. In addition, if the application is for access to a deceased's persons' record and the record contains information that the deceased person expected to remain confidential then it must remain so.

There is no obligation to advise applicants of the grounds on which information has been withheld and, if the fact that records are withheld may cause distress to the applicant, there is no obligation to notify the applicant that records have been withheld.

Once the fee is received and release agreed by the health professional then the copy of the record should be released. If the information is not readily intelligible an explanation (e.g. of abbreviations or medical terminology) must be given. The information may be withheld until the fee has been paid.

If the applicant requested to view the record then an appointment should be made. The Organisation advises that this access should be supervised. The supervision may be carried out by a lay administrator who should not comment or advise on the content of the record. If the applicant raises enquiries an appointment with a health professional should be offered.

## **18. Correcting a Record**

Under Article 16 of the DPA (2018) it provides rights to individuals to have their inaccurate personal data rectified or completed if it is incomplete (depending on the purposes for the processing). This request for rectification can be made verbally or in writing. A respond to the request must also be issued one month from receiving the request, however, there are circumstance in which a refusal for rectification may be granted.

The importance of how accurate the personal data should be, should dictate the efforts that should be put in ensuring the data is accurate.

## 19. The Information Commissioner's Office (ICO)

The ICO's office address is:

Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

ICO helpline (open between the hours of 9.00am and 5.00pm, Monday to Friday)

Tel: 08456 30 60 60 or 01625 54 57 45

Fax: 01625 524510

New or existing notification under the Data Protection Act,  
email [notification@ico.gsi.gov.uk](mailto:notification@ico.gsi.gov.uk)

Enquiries not related to legislation, email [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk).

Website <http://www.ico.gov.uk/>

Online enquiries: [http://www.ico.org.uk/for\\_the\\_public](http://www.ico.org.uk/for_the_public)

**Appendix A.**

**Log for applications to access health records by patients or their authorised representatives**

Date received	
Received by	
28 days response date	
Has the data subject been notified of extension	
Extended date given to the Data Subject	
Patient name	
Patient DOB	
Patient NHS number	
Applicant Name (if not the patient)	
Applicant Address	
Response date to applicant	

A record of the logged applications should be sent to:

Telephone:

Safe Haven Fax:

E-mail:

## Appendix B

### Current Charges

There are no current charges for subject access requests due to the new DPA (2018), requirements however, some charges can be made in the following

Circumstances:

- where further copies are requested by the data subject,
- or the request is manifestly unfounded, or excessive (definitions still required by the ICO) a reasonable fee based on the organisations administration costs may be charged

### Fees to get a copy of health records (if excessive or unfounded)

If you want a copy of the health records, the fee will depend on how the records are stored:

- on computer: maximum £10
- partly on computer and partly in another form: maximum £50
- entirely in another form: maximum £50
- The maximum charges include postage and packaging.

### Health records of someone who has died

You may have to pay a fee to view a deceased person's health records, so ask if there is a charge before you apply to see the records.

There should be no charge if the records have been updated in the previous 40 days.

If the records have not been updated in the last 40 days, the maximum charge is £10, whether the records are stored on computer or as paper-based records.

If you require copies of the records, there will be an additional charge. However, this charge should not exceed the cost of making copies and postage costs.

Only individuals nominated by the Caldicott Guardian or Deputy Caldicott Guardian are allowed to copy and process requests. All requests must go through the CCGs Responsible Officer for access to records.

## Appendix C

### Fees Received for Access to Health Records Form

Please send this form to:

To be completed by department receiving payment

Request received from:

Date (DD/MM/YYYY)

Received by Signed

Print Name

Designation Location

To be completed by Finance dept

Amount £

Budget Code:

Department:

**Appendix D**

**Form to be used when a patient requests Access to Health Records under the Data Protection Act (2018) accompanied with a proof of identification (photocopy of passport/driver's license)**

Please print all details

Full Name (including any former names)	
Date of Birth	
NHS Number (if known)	
Current Address	
Former Address(es)	

I am applying for access to view my health record / I am applying for copies of my health record (Delete as appropriate).

**Optional.** Please inform us of the period or part of your health record you require. This may include specific dates, consultant name, location, written diagnosis or certain reports.

I am applying to access my health records under the Data Protection Act 2018. I understand that under the Data Protection Act (2018) [Fees and Miscellaneous Provisions] Regulations 2001, there may be a charge for me to view, or to be provided with, a copy of my health record.

Signed.....Date.....

**Appendix E**

**Form to be used when a patient representative requests Access to Health Records under the Data Protection Act (2018). (Not to be used if patient is deceased) accompanied with a proof of identification (photocopy of passport/driver's license)**

Please print all details

Full Name (including any former names)	
Date of Birth	
NHS Number (if known)	
Current Address	
Former Address(es)	

**Optional.** Please inform us of the period or part of the patient's health record you require. This may include specific dates, consultant name, location, written diagnosis or certain reports.

I authorise (state the name of your representative:-

.....

to apply for access to my health records under the Data Protection Act (2018). I understand that under the Data Protection Act (2018) [Fees and Miscellaneous Provisions] Regulations 2001, there may be a charge for my representative to view, or to be provided with, a copy of my health record.

Signed.....Date.....

Representative's

signature.....

Print Name of representative

.....

Address to which a reply should be sent

.....

.....

.....

.....

.....

**Appendix F**

**Form to be used by a deceased person’s representative to access the deceased person’s health record under the terms of Access to Health records Act (1990).**

Full Name of Patient (including any former names)	
Date of Birth	
Date of Death	
NHS Number (if known)	
Last Address	
Former Address(es)	

**Optional.** Please inform us of the period or part of the patient’s health record you require. This may include specific dates, consultant name, location, written diagnosis or certain reports.

**Declaration please delete 1 or 2 as appropriate**

1. I am the deceased patient’s personal representative and attach confirmation of my appointment (see paragraphs 8.1 – 8.3)
  
2. I have a claim arising from the patient’s death and wish to access information relevant to my claim on the grounds that:-

Signed.....Dated .....

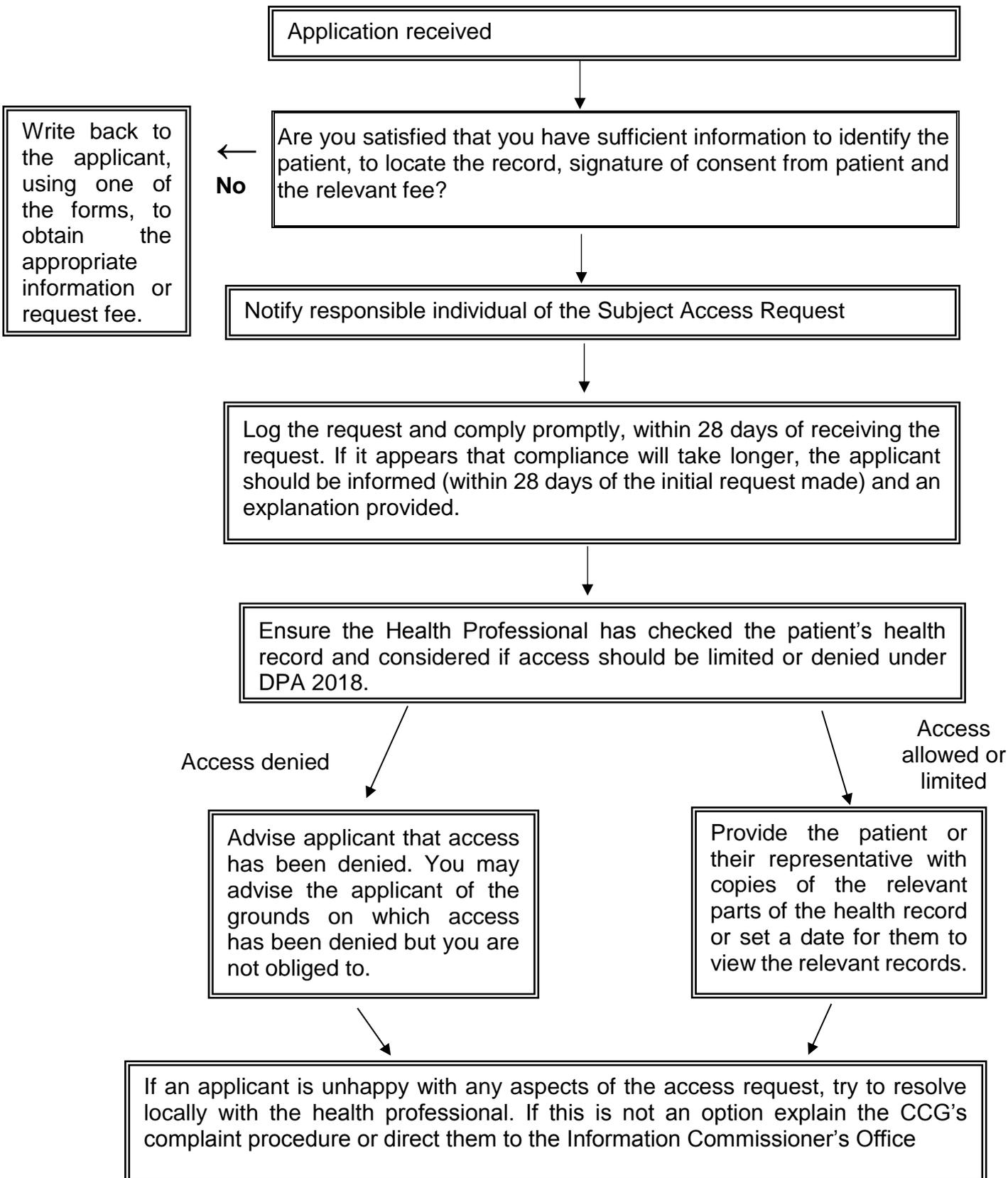
Print Your Name .....

Address to which a reply should be sent:

.....  
.....  
.....  
.....  
.....

**Appendix G**  
**Flow Chart Quick Reference Access to Health Records Checklist**

**Only the individuals nominated by the Caldicott Guardian or Deputy Caldicott Guardian can access and provide records.**



## Appendix – Contact List

Name	Position	Base	Email Address	Telephone Number
Tom Travers	Senior Information Risk Owner	Becketts House	t.travers@nhs.net	0203 182 2916
Jacqui Himbury	Caldicott Guardian	Maritime House	jacqui.himbury@nhs.net	0203 182 2918
Rob Meaker	Data Protection Officer	Becketts House	Rob.meaker@nhs.net	0203 182 3077
TBC	Information Governance Lead	Becketts House	TBC	TBC
Rebecca Bada	PSO for IG and Innovations	Becketts House	Rebecca.bada@nhs.net	0203 182 3169