



***South Sefton
Clinical Commissioning Group***

NHS South Sefton Clinical Commissioning Group

**Subject Access Request Policy
2014 - 2016**

Title:		Document Number		
NHS South Sefton CCG Subject Access Request Policy				
Next Revision Due: October 2016		Author	Consultation and Communication	Approved by
Department responsible for this document:	Cheshire and Merseyside Commissioning Support Unit (North West CSU)	Senior Governance Manager (Information Governance)	Corporate Governance Support Group	SSCCG Quality Committee
DESIGNATION	NAME	SIGNATURE		DATE
Chief Finance Officer	Martin McDowell			October 2014

Version Control:

Version History:		
Version Number	Reviewing Committee / Officer	Date
1.0	Corporate Governance Support Group	8 th October 2014
	SSCCG Quality Committee	18 th December 2014

Table of Contents

Section	Page
1. SUMMARY	4
2. KEY PERFORMANCE INDICATORS	4
3. PRINCIPLES	4
4. OBJECTIVES OF THE POLICY	5
5. RESPONSIBILITIES	5
6. SUBJECT ACCESS REQUEST GUIDANCE	7
7. SUBJECT ACCESS REQUESTS: PROCESS OF ADMINISTRATION	18
8. HOW DO I REQUEST INFORMATION HELD ABOUT ME?	18
9. MONITORING	19
10. EQUALITY IMPACT ASSESSMENT	19
11. ASSOCIATED DOCUMENTS	19

1. SUMMARY

- 1.1. The Subject Access Request Policy for the CCG sets out the requirements of its staff for managing requests to access records. In general terms, this Policy covers all records, which do or could identify an individual for which the CCG 'holds' information.
- 1.2. The Information Governance Strategy, and the policies associated with it, should be read together.
- 1.3. Activity reports on the Subject Access Request applications will be produced for the CCG Officers appropriate meeting.
- 1.4. This policy covers 'Subject Access Requests' (SARs) under the terms of the Data Protection Act 1998, section 7. The CCG deals with two categories of Subject Access Requests:
 - Access to health related records e.g. patient complaint.
 - Other Subject Access Requests e.g. staff personal records.
- 1.5. Cheshire and Merseyside Commissioning Support Unit (hereafter referred to as the CSU) will manage the requests on behalf of the CCG.

2. KEY PERFORMANCE INDICATORS

- 2.1. The following key performance indicators have been identified to measure the effectiveness of this document:
 - i. annual Information Governance Toolkit scores;
 - ii. staff will know who and where to direct Subject Access Request applications to;
 - iii. percentage of incidents / complaints that might contravene the policy.

3. PRINCIPLES

- 3.1. The Access to Health Records Act 1990 has now been repealed, except for the sections dealing with requests to records relating to the deceased.
- 3.2. The Data Protection Act 1998 is applicable to requests for access to records relating to living persons.
- 3.3. Under the Data Protection Act 1998, individuals have the right to:

- Access their records, subject to certain safeguards.
 - Have copies of their records.
 - Have these records explained if they are illegible or unintelligible.
 - Be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.
- 3.4. Applications under The Data Protection Act 1998 cover all media, e.g. paper and computer records, including digital images and any type of voice recording.
- 3.5. Applicants do not have to give a reason for requesting access to records. The applicant's motives in requesting the records are irrelevant.
- 3.6. The 'subject' could be a patient, contractor, member of staff or member of the public.

4. OBJECTIVES OF THE POLICY

The objectives of this Policy are to:

- 4.1. Ensure that the CCG meets its obligations regarding 'subject access requests' under the terms of the Data Protection Act 1998.
- 4.2. Set out clear guidelines for CCG staff to help make the access timely and within the legislation laid down by the Government.
- 4.3. Ensure that all staff are aware of their responsibilities in the management of access to records.

5. RESPONSIBILITIES

5.1 The **Accountable Officer** of the CCG shall have overall responsibility for the Subject Access Request Policy, by ensuring that all staff within the CCG:

- comply with legislation, guidelines and procedures as set out and agreed within the Policy.
- work within the time scales set out within the Policy.

5.2 **The CCG Caldicott Guardian is responsible for:**

- Ensuring that patient information may only be passed on for a justifiable purpose and where possible only minimum information about the *patient* should be used.

5.3 The CCG Senior Information Risk Owner (SIRO) is responsible for:

- Ensuring that Person Identifiable Data (PID) and other information may only be passed on for a justifiable purpose and where possible only minimum information about the *person* should be used.

5.4 Chief Officers (CCG) are responsible for:

- Ensuring that all staff follow the process by sending the photocopies of requested information to them for the ultimate decision and signature.
- Ensuring that all Staff are aware of their accountability for any decision to pass on Person Identifiable Information (PID).

5.5. CSU Information Governance Manager is responsible for:

- Ensuring all local procedures within the CSU Customer Solution Centre and the wider CSU will meet the requirements as set out in the Data Protection Act 1998.
- Providing expert advice on the managements of SARs.

5.6. Customer Solution Centre Staff are responsible for:

- Ensuring all requests are acted upon in a timely manner as set out in the Data Protection Act 1998.
- Ensuring all consent forms are received with accompanying identification documentation.
- Ensuring that the appropriate CCG Officer has signed the Permission and Confirmation section of the request for release of records.
- Ensuring that the only documentation sent out relates to the CCG.
- Ensuring that all application monies received are recorded and banked.
- Ensuring that all applicants, including solicitors, receive acknowledgement of monies received.
- Ensuring a database of all requests is kept up to date and accurate.

5.7. CCG Senior Staff are responsible for:

- Ensuring all staff are made aware of the Subject Access Request Policy and the associated procedures.

- Ensuring all new staff receive training / guidance in security and confidentiality when dealing with confidential / sensitive records.
- Ensuring that the relevant documentation requested is made available.
- Ensuring that all staff are adequately trained and adhere to the guidelines.
- Ensuring that staff report any incidents or concerns about any aspect of confidentiality and security, whether a breach has taken place or a 'near miss' regarding Subject Access Requests on the DATIX electronic incident reporting system.

5.8. CCG Staff are responsible for:

- Ensuring awareness of the Subject Access Request Policy and following the correct procedure as set out in this policy when receiving an access request.
- Ensuring the disclosure of information is carried out as laid down in the Subject Access Request Policy.
- Ensuring awareness of responsibilities to safeguard personal data and sign an undertaking that they will abide by the requirements of the organisations Data Security Policy. In order to do this staff should be given clear guidance on how to handle confidential information in all the different media used by the CCG, including electronic and paper records.
- Ensuring awareness of the clear guidance in place locally to report any incidents or concerns about any aspect of confidentiality and security, whether a breach has taken place or a 'near miss' has occurred using the CCG DATIX electronic incident reporting system.

6. SUBJECT ACCESS REQUEST GUIDANCE

6.1. The CCG has the following guidance for managing requests.

6.2. Who Has A Right to Apply?

6.2.1. A patient

6.2.2. Any person authorised in writing, to apply on behalf of the patient (see below also).

In England and Wales, the person having parental responsibility for a child under 16 if the child agrees. If the child is competent of understanding the application, his/her consent is needed to allow access to the records, unless, in exceptional circumstances, the record holder considers that it is in the child's best interest to allow access without their consent i.e. There

is a real justification for allowing access without consent. If the child is not capable of understanding the application, the person with parental responsibility has a right of access, subject to the usual safeguards/examples.

- 6.2.3. A child (a person under the age of 16 years) who, in the view of the appropriate Healthcare Professional, is capable of understanding what the application is about can prevent a parent from having access to the record. If the child is not capable of understanding the application, the person with parental responsibility has a right of access, subject to the usual safeguards/examples, unless, in the view of the appropriate Healthcare Professional this would not be in the child's best interest, then the holder of the records are entitled to deny access (see below also).
- 6.2.4. Any person appointed by the Court, to manage the affairs of a patient of any age, who is deemed to be incapable (see below also).
- 6.2.5. Where a patient has died the patient's personal representative or any person having a claim arising from the death. Where the patient has died, disclosure would be subject to the recorded wishes of the deceased patient (see below also).
- 6.2.6. Where the applicant is not the patient, the applicant should have access to only the information which would otherwise have been available to the patient, unless access to further information is deemed justifiable in the circumstances, other than in exceptional circumstances such circumstances may arise, which, exceptionally, would justify disclosure. **Where the applicant is not the patient, access is not permitted where the holder of the records are of the opinion that the patient gave the information or underwent the examination / investigation in the expectation that the information would not be divulged to the applicant.**
- 6.2.7. The applicant must declare that they are entitled to apply for access to the health records referred to. The applicant may also give their authority to a Solicitor or anyone else they choose, to obtain copy records of the patient, on behalf of the applicant.
- Further enquiries may be needed to confirm the bona fides of applicants other than the patient before access is given. *NB proof of identification may be required for access.*
- 6.2.8. If the applicant is acting on the patient's behalf then it must be established in what capacity they are making the application.

6.3. Requests from the Police

- 6.3.1. Under the Data Protection Act 1998, Section 29.3 is an exemption in Law for the Police to get information without seeking the consent of the individual(s) for crime & taxation purposes.
- 6.3.2. The Police have a form specifically for this. It is referred to as a 'section 29.3 form' which allows them to approach any data controller (the CCG in this case) for information regarding an individual, in relation to the apprehensive of an offender (may or may not be the same person) or for the prevention of a crime, or for the prosecution of a crime.
- 6.3.3. If the Police can show that the information is needed to further their case (and this would be set out on the section 29.3 form), they can receive it.
- 6.3.4. A section 29.3 form is the safe guard to the data controller for releasing the information to the Police, in case of any objection by the data subject.
- 6.3.5. If the CCG do not accept whatever the Police put on the 'section 29.3 form', the Police would have to seek a court order to subpoena the CCG to submit the file/information to Court for a Judge to rule on disclosure.

6.4. Records for Patients under the Age of 16

- 6.4.1. The applicant must have parental responsibility. This will be by way of one of the following:
- 6.4.2. The applicant is the child's natural mother (and there are no residents or other Court Order to the contrary). We have to take the applicants / Solicitors written word for this at face value. This is often referred to as *acting in loco parentis* and is where the patient is under age 16 and is incapable of understanding the request.

Also

Where the patient is under age 16 but is mature enough to understand the meaning of the application and giving authority (*termed as being Frazer Competent*) and has consented to the applicant making this request, the authorisation of the patient and / or mother should be given. Again, we have to take the applicants / Solicitors written word for this at face value.

- 6.4.3. The applicant is the child's natural father and was married to the child's natural mother at the time of conception or birth of the child. NB the father does not necessarily still have to be married to the child's natural mother. He could be legally separated or divorced from her. Also, this whole point only applies providing that there is no residence or other Court Order to the contrary. We can accept Solicitors written confirmation of this. Marriage / Divorce papers are not necessary.

- 6.4.4. The applicant is the child's natural father but was not married to the child's natural mother at the time of conception or birth of the child, but there is an agreement between both parents, which has been passed by a Court of Law, expressly giving the natural father parental responsibility. Documentation will exist if this is the case, and a photocopy of it should be obtained. Since December 2003 if mother agrees an unmarried father has parental rights if the child registered together and fathers name goes on the Birth Certificate.
- 6.4.5. The applicant has parental responsibility by way of a Residence Order. This could be the child's natural father, a grandparent or other relative. Documentation will exist if this is the case, and a photocopy of it should be obtained. NB a Residence Order is not time limited – up to their sixteenth birthday unless discharged.
- 6.4.6. If the applicant does not satisfy any of the above criteria, then access to the records will be denied, unless the applicant can provide the written authority of someone who has got parental responsibility.

6.5. Records for Patients over the Age of 16

- 6.5.1. Patients capable of managing their own affairs - the applicant must have the written authority of the patient if they are capable of managing their own affairs.
- 6.5.2. Patients incapable of managing their own affairs - the applicant must have proof that they have the authority to act on behalf of the patient. This will be by way of one of the following:
- 6.5.3. They have been appointed by the Court to manage the patient's affairs. Documentation will exist if this is the case, and a photocopy of it should be obtained.
- 6.5.4. They are the deceased patient's personal representatives. Documentation will exist if this is the case, and a photocopy of it should be obtained.

6.6. Other Considerations for All Records for Patients of Any Age

- 6.6.1. A Healthcare Professional has also got the discretion to release records to an applicant if they consider it to be in the best interests of the patient at that time and there is an overriding public interest justification why the records should be released without the authority of the person entitled to access the records. They would be responsible for their clinical judgement. A good example of this would be in a case of child sexual abuse.
- 6.6.2. A patient's dental or other such records that would be needed for purposes of identification can be released at the request of a written request from the

Coroner, a signature acknowledging receipt of such records must be provided on the appropriate form. This must be recorded and dated as per Access to Health Records.

- 6.6.3. The only other over riding rule would be if a Solicitor or the Police gained a Court Order for the organisation to release the records to the Court. The organisation would then have no choice in the matter and the Judge would decide whether or not the records should go to the Solicitor / Police / applicant.
- 6.6.4. Special permission may also be given when the interests of the public are thought to be of greater importance than the patient's confidentiality. This is very rare, but some situations where this might happen include:
 - 6.6.5. When a serious crime has been committed;
 - 6.6.6. When there are serious risks to the public or NHS staff;
 - 6.6.7. To protect children
- 6.6.8. This permission is given by the Caldicott Guardian in charge of protecting privacy in each health care organisation.
- 6.6.9. Special permission will be given to use patient health records without consent e.g. medical research, keeping registers of cancer patients or checking quality of care. This permission is given by the National Information Governance Board (NIGB). This would be under section 251 of the NHS Act 2006.

6.7. When Access to Records may be denied or Partially Excluded

- 6.7.1. Within the Act there is provision for some information to be withheld:
- 6.7.2. The patient does not have to be told that information has been withheld because that in itself could be damaging to them.
- 6.7.3. The patient is not, however, prevented from asking the practitioner whether the full record has been made available, and may apply to the Courts if they are dissatisfied with the answer.
- 6.7.4. The fact that a record has not been prepared in anticipation that it might be opened is no justification for denying access. Also, fear of legal action is not a reason for denying access.
- 6.7.5. Healthcare Professionals are advised that records should be compiled on the assumption that they will be opened to patients and / or the Courts.
- 6.7.6. Access shall not be given unless the holders are satisfied that the applicant is capable of understanding the nature of the application and the meaning of the authorisation.

- 6.7.7. Where a patient has died, access should not be given to the (records / information), which in the opinion of the holder is not relevant to any claim arising out of the death. Also, if the patient has died and the record includes a note made at the patient's request that he / she did not wish access to be given to their personal representative or to any person having a claim arising from their death, access will be refused.
- 6.7.8. Access can be denied if the disclosure of information would cause serious harm to the physical or mental health or condition of the patient or any other person or if disclosure would go against the wishes of the patient unless, in exceptional circumstances, disclosure is justified even though it may go against the patient's wishes. Such circumstances would be very exceptional.
- 6.7.9. This generally refers to severe mental illness, malignancy and degenerative neurological conditions.
- 6.7.10. Where information that is adjudged to be harmful is withheld, an appointment should be made for the applicant to inspect the remainder of the record with the Healthcare Professional.
- 6.7.11. Where the records contain personal information relating to third parties unless the third party is a doctor or other Healthcare Professional who has compiled or contributed to the record or has been involved in the care of the patient in his/her capacity as a Healthcare Professional, unless their consent has been given, access shall not be given, e.g. a family member (see below also).
- 6.7.12. Where the application is on behalf of a child or a person incapable of managing his or her own affairs or where a patient has died, access may not be given to information as a result of examination or investigation where the expectation was that the information would not be disclosed.

6.8. Third Party Information

- 6.8.1. Where the third party has consented to the disclosure to the person making the request, the appropriate Manager is obliged to comply with the request and disclose the third party information.
- 6.8.2. However, consent may not have been given for one or more reasons, examples of which are:
- 6.8.3. Consent has not been sought.
- 6.8.4. It is not possible to obtain consent because the third party's whereabouts are unknown.
- 6.8.5. The third party does not have legal capacity to consent.

- 6.8.6. The third party declines to consent.
- 6.8.7. Where consent has not been given (for whatever reason), the appropriate Manager is nevertheless required by the subject, access provisions to comply with the request and disclose third party information if it is reasonable in all the circumstances to disclose without consent. However, to avoid falling foul not only of the Act, but other provisions of law, e.g. confidentiality, disclosure without consent should not be made until proper consideration has been given to all relevant factors. The Act highlights some of the factors to be taken into account in deciding this, but the list is not exhaustive:
- 6.8.8. Any duty of confidence owed to the third party.
- 6.8.9. Any steps taken by the appropriate Manager to seek the consent of the third party.
- 6.8.10. Whether the individual is capable of giving consent.
- 6.8.11. Any express refusal of consent by the other individual.
- 6.8.12. The appropriate Manager may at the very least need to take steps to seek consent in order to demonstrate that it was reasonable in the circumstances to make the disclosure without consent.

6.9. Time Limits for Access

- 6.9.1. The Act imposes very specific duties upon us, which have to be carried out within a very tight timescale. From receipt of the application form, 14 days are allowed if the record holder needs more information, either to identify the record(s) asked for, or to check the identity of the person applying for access.
- 6.9.2. The information is to be supplied within 40 days from the date of the request for access or within 40 days from the date you have sufficient information to enable you to satisfy yourself as to the identity of the person making the request and to locate the information requested.
- 6.9.3. However, the Department of Health states that National Health Service bodies should endeavour to comply with subject access requests within 21 calendar days. The Information Commissioner has also stated that requests should be complied with within 20 working days in accordance with the Freedom of Information Act 2000.
- 6.9.4. ***Failure to comply gives the applicant a right of action in the County Court or High Court. It is therefore essential that all applications be processed as a matter of priority, thereby minimising risk to the organisation.***

6.10.Charging for Subject Access

- 6.10.1. A maximum fee of £50 may be charged for granting access to manual records, or to a mixture of manual and automated records, where the request for subject access will be granted by supplying a copy of the information in permanent form. However, for granting access to health records that are only being automatically processed, or that are recorded with the intention that they be so processed, a fee of £10 may be charged.
- 6.10.2. A charge of 40p per photocopied side of paper would be reasonable, plus any postage costs. It should be noted that there is no express provision for any fee to be charged for copying or despatching copies of records.
- 6.10.3.No fee may be charged where the access request is to be complied with other than by supplying a copy of the information in a permanent form, i.e. by allowing the applicant to inspect the record. This provision only relates to requests for access to non-automated manual records, at least some of which were made after the beginning of the period of 40 days immediately preceding the date of the request. This provision broadly replicates the provision of the Access to Health Records Act 1990 that, in effect, allows patients to look at recently created records for free.

6.11.Mistakes or Inaccuracies

- 6.11.1. If the applicant considers that there are mistakes or inaccuracies in the record they can ask the record holder for a note to be made in the records stating their opinion. If the practitioner agrees that the information is inaccurate, he / she should make the correction. Care must be taken not to simply obliterate information, which may have significance for the future care and treatment of the patient, or for litigation purposes.
- 6.11.2. If he /she does not agree, a note recording why the applicant considers the information to be inaccurate must be made in the relevant part of the record. Consideration should also be given to whether it is appropriate to note any associated records, e.g. computer records.
- 6.11.3. It should be understood that in Law nothing may be erased from a paper health record but a correction may be added.
- 6.11.4. A copy of any correction or note should be supplied to the patient. No fee may be charged for this.

6.12.Complaints Concerning Application

- 6.12.1. If the applicant feels that they have not been fairly treated and that the holder of the record has not complied with the Act, then they should first complain in writing to the Chief Clinical Officer of the CCG.
- 6.12.2. If they are still unhappy after this, the applicant has the right to apply to the Information Commissioner to review the outcome of the application if necessary. To complain to the Information Commissioner, please see the ICO web page at: <http://www.ico.gov.uk/complaints/getting/complain.aspx>

6.13. Additional Information

- 6.13.1. Requests for access to information may be made in some circumstances under the Freedom of Information Act 2000. Please see the Freedom of Information section of our website to make a request for corporate information.

6.14. Requests for Personal Data - the Freedom of Information Act and Data Protection Act

- 6.14.1. The Personal Data Exemption in the Freedom of Information Act 2000 falls under Section 40. Section 40 provides an exemption from the right to know principle where the information requested by an applicant consists of personal data. You would think that this means that all requests for access to personal data, including medical records, would fall under the Access to Health Records Act or Data Protection Act respectively. However, the exemption is phrased in such a way that this is not the case.
- 6.14.2. Regarding access to information relating to deceased persons, it is important to note that the definition of 'personal data' in Section 40 is restricted to information relating to living individuals. Information, which relates solely to a deceased person, is not covered by this exemption. Section 40 will only apply if the information relating to the deceased person is also the personal data of a living individual. For example, genetic information about a deceased person may also be the personal data of that person's ancestors and descendants. If the information requested relates solely to a deceased person, the information is potentially disclosable under the Freedom of Information Act.
- 6.14.3. However, other exemptions in the Freedom of Information Act may be applicable to personal information relating to deceased persons and may justify a refusal to disclose under the Act. For example; Section 21, which exempts information readily accessible to the applicant by other means - section 3 of the Access to Health Records Act 1990 allows a deceased patient's personal representative or anybody who may have a claim arising out of the death to access the patient's health records; Section 38, which exempts information whose disclosure would or would be likely to

endanger the physical or mental health or the safety of any individual (for example by means of shock or distress); Section 41, which exempts information obtained by a public authority from another person if the disclosure of this information to the public would constitute a breach of confidence actionable by that or another person; Section 44, which exempts information where disclosure is prohibited by or under any enactment, including the Access to Health Records Act 1990 and the Human Rights Act 1998. If disclosure of information relating to a deceased person would breach the right to a private and family life of a living person (as protected by Article 8 of the European Convention on Human Rights), it will be exempt under Section 44 because it would breach section 6 of the Human Rights Act.

6.15. The Application of the Section 40 Exemption (Freedom of Information Act) to Information Relating to Living Individuals

- 6.15.1. If the personal data requested relates to the applicant, then the request should be treated as a subject access request under the Data Protection Act, as usual. This would also cover the situation whereby the request is made by a Solicitor on behalf of his client, a parent on behalf of a child, a person appointed by the Court on behalf of a person who lacks capacity etc, because these are all still subject access requests i.e. requests made by a person with authority to make the request on the data subject's behalf.
- 6.15.2. The Information Commissioner Guidance says that, whilst such a request is to be treated as a request under the Data Protection Act, you should inform the applicant if you will be unable to respond within the Freedom of Information Act 20 working day period and require the 40 calendar day period allowed under the Data Protection Act instead. The Department of Health has stipulated that the NHS should endeavor to comply with subject access requests within 21 days, rather than the allowed 40 days - this is not legislation, just guidance. Access to Health Records will aspire to comply within the 21-day or, at least, 20 working day timescale under the Freedom of Information Act, and if this is not possible, the applicant should be informed that the request will be dealt with (within 40 calendar days) under the Data Protection Act.

6.16. If the Information Requested Relates to a Third Party

- 6.16.1. If the personal data requested is about somebody other than the applicant (the above exceptions of solicitor, parent, etc aside), the exemption under the Freedom of Information Act will only apply if disclosure would breach any of the Data Protection Principles. So, the usual data protection rules apply as to when it would be justifiable to disclose without consent and when it would not be - if disclosure would breach the usual data protection rules, disclosure need not take place. However, if disclosure is justified in accordance with the usual Data Protection rules, it can take place and the

fees structure and timescale under the Freedom of Information Act should apply. Whilst the following does not directly apply to medical records, it is interesting to note that the Information Commissioner's Guidance states that information relating to somebody acting in an official or work capacity should normally be provided on request, unless there is a risk to the individual concerned – 'the exemption from disclosure should not be used as a means of sparing officials embarrassment over poor administrative decisions'!

- 6.16.2. Under the Access to Medical Reports Act 1988, individuals can apply to access medical reports prepared for employment or insurance purposes.
- 6.16.3. The Secretary or State may make further orders to exclude other types of data if this is necessary to safeguard the interests of Patients or the Rights and Freedoms of others.
- 6.16.4. In most cases access under the Act will be straightforward. However, there will be instances where a detailed knowledge of the Act and its implications are vital.
- 6.16.5. The Information Commissioners websites provide some useful information:
<http://www.ico.gov.uk/>
- 6.16.6. Any further advice should be directed to the Solicitors acting for the CCG, for which permission from a Senior Officer must be first agreed.

6.17. Subject Access Request Definitions

- 6.17.1. There are certain definitions given in the Act. These are:

An **application** means an application in writing (see Process of Administration below).

A **health record** is defined as information relating to the physical and / or mental health of an individual who can be identified from that information and which has been made by, or on behalf of a Healthcare Professional, in connection with the care of that individual.

The **holder** of the record is the CCG by which, or on whose behalf, the record is held.

The **patient** is the individual in connection with whose care the record has been made.

The **Healthcare Professional** can be one or more registered health professionals.

7. SUBJECT ACCESS REQUESTS: PROCESS OF ADMINISTRATION

- 7.1 There are certain procedures that must be observed when applying to see records under the Act. It may seem a rather complicated process but it is of vital importance to make sure that the records are released only to the right person, because the confidentiality of records calls for the greatest safeguards.
- 7.2 Any member of staff receiving a formal request for access, either verbally or in writing should advise the person to obtain an application form from the CSU Customer Solution Centre, or from the CSU or CCG website.
- 7.3 The CSU Customer Solution Centre will manage the request in line with the CSU Process Centre Manual.

8. HOW DO I REQUEST INFORMATION HELD ABOUT ME?

- 8.1 The Data Protection Act allows you to find out what information the NHS holds about you, as a patient, on computer and in some paper records. This is known as the 'right of subject access'.
- 8.2 A request for information from a health record has to be made with the appropriate Data Controller, this will be your GP or relevant hospital trust where you were treated.
- 8.3 NHS England is only the data controller of GP health records where an individual is currently not registered with a GP or is deceased. For access to GP health records in these circumstances [please use the list here](#) to direct the request to the appropriate service (the list is by the geographical area of the GP).

9. MONITORING

- 9.1 Compliance with this Policy will be monitored via the CCG SIRO, CCG Caldicott Guardian, the Information Governance Senior Manager (CSU), together with independent reviews by both Internal and External Audit on a periodic basis.
- 9.2 The Information Governance Senior Manager is responsible for the monitoring, revision and updating of this Policy on a 2 yearly basis or sooner if the need arises.
- 9.3 This Policy will be made available to all Staff via the CCG Intranet site.

10. EQUALITY IMPACT ASSESSMENT

- 10.1. This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.
- 10.2. As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

11. ASSOCIATED DOCUMENTS

The following documents will provide additional information:

- Information Governance Strategy
- Information Governance Policy
- Confidentiality and Data Security Policy
- Freedom of Information Policy
- Corporate Records Management and Retention Policy
- The suite of ICT security policies