Subject Access Request Policy

2017

**Important:** This document can only be considered valid when viewed on the CCG’s website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

<table>
<thead>
<tr>
<th>Name of Policy:</th>
<th>Subject Access Request Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Issued:</td>
<td>November 2017</td>
</tr>
<tr>
<td>Date to be reviewed:</td>
<td>2 years from approval date</td>
</tr>
<tr>
<td>Policy Title:</td>
<td>Subject Access Request Policy</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Supersedes: (Please List)</td>
<td>Subject Access Request Policy v1.1</td>
</tr>
<tr>
<td>Description of Amendment(s):</td>
<td>Addition of DH Guidance re applications from those who cannot put a request in writing.</td>
</tr>
<tr>
<td></td>
<td>Addition of reference Materials</td>
</tr>
<tr>
<td></td>
<td>Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).</td>
</tr>
<tr>
<td>This policy will impact on:</td>
<td>All Staff</td>
</tr>
<tr>
<td>Financial Implications:</td>
<td>No change</td>
</tr>
<tr>
<td>Policy Area:</td>
<td>Data Protection</td>
</tr>
<tr>
<td>Version No:</td>
<td>1.2</td>
</tr>
<tr>
<td>Author:</td>
<td>Yorkshire and Humber CSU IG Team</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>November 2017</td>
</tr>
<tr>
<td>Review Date:</td>
<td>October 2019</td>
</tr>
<tr>
<td>Impact Assessment Date:</td>
<td>Complete</td>
</tr>
</tbody>
</table>

**APPROVAL RECORD**

<table>
<thead>
<tr>
<th>Integrated Audit and Governance Committee</th>
<th>08 March 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Audit and Governance Committee</td>
<td>November 2017</td>
</tr>
</tbody>
</table>

**Consultation:**

| Members of SLT | 18 January 2016 |
Policies Amendments

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

<table>
<thead>
<tr>
<th>New Version Number</th>
<th>Issued by</th>
<th>Nature of Amendment</th>
<th>Approved by &amp; Date</th>
<th>Date on Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Barry Jackson</td>
<td>Approved version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Helen Sanderson</td>
<td>Addition of DH Guidance re applications from those who cannot put a request in writing.</td>
<td>Integrated Audit and Governance Committee – November 2017</td>
<td>November 2017</td>
</tr>
<tr>
<td>1.2</td>
<td>Mark Culling</td>
<td>Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).</td>
<td>Integrated Audit and Governance Committee – November 2017</td>
<td>November 2017</td>
</tr>
<tr>
<td></td>
<td>CONTENTS</td>
<td>Page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Introduction &amp; Applicability</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Engagement</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Impact Analyses</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.1 Equality</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.2 Sustainability</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Scope</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Policy Purpose and Aims</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Implementation</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Training and Awareness</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Monitoring and Audit</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Reporting Security Incidents and Assurances from IT Suppliers</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Policy Review</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Annex A</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Annex B</td>
<td>17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1 INTRODUCTION AND APPLICABILITY

1.1. Individuals have the right under the Data Protection Act 1998, (to be superseded by the General Data Protection Regulation (GDPR) on 25th May 2018), subject to certain exemptions, to have access to their personal records that are held by Hull Clinical Commissioning Group (The CCG). This is known as a ‘subject access request’ (SAR). Requests may be received from members of staff, service users or any other individual who the CCG has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

1.2. Anyone making such a requested is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, where the information was gathered from. Under GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or raise and objection to the processing altogether.

1.3. The Data Protection Act 1998 (and GDPR) applies only to living persons but there are limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990.

1.4. The CCG has developed this policy to guide staff in dealing with Subject Access Requests that may be received.

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

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

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 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.

As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

4 SCOPE

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this procedure applies to all third parties and others authorised to undertake work on behalf of the CCG.

The purpose of this procedure is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests.

5 POLICY PURPOSE & AIMS

5.1 What is a Subject Access Request?

1. A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information about them, which is held by the CCG. The Data Protection Act (DPA) 1998 (Section 7) (to be superseded by the General Data Protection Regulation (GDPR) on 25th May 2018) entitles all individuals to make requests for their own personal data. An individual is not entitled to information relating to other people (unless they are acting on behalf of that person).

The request does not have to be in any particular form other than in writing, nor does it have to include the words ‘subject access’ or make any reference to the Data Protection Act 1998 (to be superseded by the General Data Protection Regulation (GDPR) on 25th May 2018). A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore be treated as a SAR in the normal way. The applicant must be informed of how the application is being dealt, under which legislation and of any fees applicable.

Where an individual is unable to make a written request it is the Department of Health view that in serving the interest of patients it can be made verbally, with the details recorded on the individual’s file.
2. Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:
   • told whether any personal data is being processed;
   • given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
   • given a copy of the personal data; and
   • given details of the source of the data (where this is available).

3. Personal data is information that relates to an individual who can be identified either directly or indirectly and includes any expression of opinion about the individual and any indication of the intentions of the information holder or any other person in respect of the individual. Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR.
   • All clinical data should be reviewed by a clinician and consideration should be given to redacting any information likely to cause serious harm to the mental or physical health of any individual
   • Information supplied by third parties e.g. family members should usually be redacted
   • Data and information held from other agencies may be disclosable but should be discussed with the originating body first
   • Any information subject to Legal Professional Privilege should not be disclosed
   • Information should not be disclosed where there is a statutory or court restriction on disclosure e.g. adoption records
   • References written for current or former employees are exempt (but not those received from third parties)
   • In the case of deceased records, information should not be disclosed where the entry in the records makes it clear that the deceased expected the information to remain confidential
   • A personal record may also contain reference to third parties and redaction should be considered by balancing the Data Protection rights of all parties

5.2 How to recognise and action a Subject Access Request

1. In order for the CCG to action a subject access request the following must be received:
   • The request must be made in writing (This may be by letter, fax, email, or even social media, such as facebook or twitter). It is important to note that responses to SAR requests must be returned by a secure methodology, i.e. social media must NOT be used to return information requested. However where the applicant is not able to make the request in writing it can be received verbally and a record of the request made on the applicants file or it can be written in their file.
   • Any fee levied, as deemed appropriate, this may be waived (information must be provided free of charge under GDPR from 25th May 2018).
   • Proof of identity of the applicant and/or the applicant representative, and proof of right of access to another person’s personal information.
   • Sufficient information to be able to locate the record or information requested.
   Requests should be dealt with within a maximum of 40 calendar days (maximum of one month under GDPR) subject to the necessity to seek clarification or collect any fee payable. Under GDPR it is possible to extend this timescale by a further two months where
requests are complex. However if this is the case the CCG must inform the individual within one month of the request and explain why the extension is necessary. NHS best practice recommends disclosure within 21 days where a record has been added to in the last 40 days. 2. If the request relates to, or includes information that should not be requested by means of a SAR (e.g. it includes a request for non-personal information) then, the request must be treated accordingly, e.g. as a FOI request where purely non-personal data is being sought or as two requests: one for the requester’s personal data made under the DPA; and another for the remaining, non-personal information made under FOIA. If any of the non-personal information is environmental, this should be considered as a request made under the EIR.

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

4. All SAR requests received must be forwarded to the relevant head of department, e.g. staff requesting access to personnel records must be sent to Head of HR, without delay in order for it to be processed within the legal timescale.

5. The Common Law Duty of Confidentiality extends beyond death. Certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:

   o The patient’s personal representative (Executor or Administrator of the deceased’s estate)
   o Any person who may have a claim arising out of the patient’s death

6. A Next of Kin has no automatic right of access but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from the Caldicott Guardian in relation to requests for deceased records

5.3 Assisting and Advising Service Users on how to make a request.

1. Where an individual is verbally making a request you should advise that the will need to:

   • Put the request in writing, detailing the information they are requesting and from which service to enable it to be located.

   • Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request.

   • A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure that you and your colleagues can recognise a SAR and deal with it in accordance with this procedure and forward immediately to the relevant service head.
Advise the applicant to send the request to the appropriate head of service, and provide contact details.

In order to comply with equality legislation, where an applicant is unable to put the request in writing assistance should be given to them to make the request verbally, best practice would be to document the request details in an accessible format for the applicant and request them to confirm the details are correct. Applicants can be referred to the Patient Relations Team to obtain appropriate assistance in making their application.

Note that responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed e.g. braille.

5.4 Requests made about or on behalf of other individuals

General Third Party

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

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

Requests on Behalf of Children

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

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child’s treatment plan is confident that the child can be considered competent under Gillick/Fraser guidelines, has the capacity to understand their rights and any implications of the disclosure of information, then child’s permission should be sought to action the request. Further guidance is expected in relation to the rights of children under GDPR.

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

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

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

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

4. Access Requests for those who lack capacity to consent

In certain circumstances a person acting as an advocate can seek access to personal information in so far as it is necessary or relevant to their role. This includes:

- Persons appointed by the Court of Protection
- Persons holding a registered Power of Attorney for specified purposes
- Persons appointed as Independent Mental Health Advocates under the Mental Capacity Act 2005

5. Remote Access to Records

- Under GDPR, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

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

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

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

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

A formal documented request signed a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.
These types of requests must be considered by a senior manager and the decision on whether to share the information or not documented before any action is taken. Advice can be sought from the Information Governance Team.

**Court Orders**

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

**5.5 Responding to requests**

It is essential that a log of all requests received is maintained, detailing:
- Date received
- Date response due (within 40 calendar days of receipt (maximum of one month under GDPR)
- Applicants details,
- Information requested,
- Any fees levied (information must be provided free of charge under GDPR from 25th May 2018),
- Exemptions applied in respect of information not to be disclosed,
- Details of decisions to disclose information without the data subjects consent,
- Details of information to be disclosed and the format in which they were supplied,
- When and how supplied, e.g. Paper copy and postal method used to send them.

1. Determine whether the person’s request is to be treated as a routine enquiry or as a subject access request. If you would usually deal with the request in the normal course of business, e.g. confirming appointment times or details of public meetings planned then do so. The following are likely to be treated as formal subject access requests.
   - Please send me a copy of my HR file or Medical Records.
   - I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed.
   - The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.

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

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

In the case of requests for clinical records these should be reviewed by the Caldicott Guardian or a nominated representative who shall decide to what extent data can be disclosed or whether the request is to be refused.
Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual. However information contained within the information requested was supplied by health professionals it may be disclosed without consent if considered appropriate.

4. Determine whether a fee (not applicable under GDPR from 25th May 2018) is to be charged, this does not have to be applied. Where fees are to be applied the maximum this can be is £10 or up to maximum of £50 for medical records in a permanent format, however this is to be assessed on a sliding scale. e.g.
   - Fewer than 20 Pages £1
   - Under 30 £2
   - Under 40 £3 Etc
   - When the number of pages exceeds 500 only then will the maximum fee of £50 apply.

   A reasonable fee may be charged under GDPR for any further copies of the information or when a request is manifestly unfounded or excessive, but any fee must be based on administrative costs only. It is possible to refuse to respond to manifestly unfounded or excessive requests under GDPR but the CCG must explain to the individual of their right to complain to the Information Commissioner’s Office as soon as possible and at the latest within one month.

   Further details can be found at: Access to Records Fees Regulations 2000

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

6. It must be determined whether the information is likely to change between receiving the request and sending the response. Routine on-going business additions and amendments may be made to the personal information after a request is received, however the information must not be altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under the Data Protection Act 1998 (to be superseded by the General Data Protection Regulation (GDPR) on 25th May 2018).

7. Check whether the information collated contains any information about any other individuals and if so, consider:
   - Is it possible to comply with the request without revealing information that relates to the third party?
     (Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party)
     Where it is not possible to remove third party identifiers you must consider the following.
     - Has the third party consented to the disclosure?
     - Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party?
     (The following must be considered when trying to determine what reasonable circumstances are);
     - duty of confidence owed to the third party,
     - steps taken to try and obtain consent,
     - whether the third party is capable of giving consent, and
     - any express refusals of consent from the third party.
A record of the decision as to what third party information is to be disclosed and why should be made.

8. Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:
   - Crime prevention and detection, including taxation purposes,
   - Negotiations with the requestor,
   - Management Forecasts,
   - Confidential References given by you,
   - Information used in research, historical or statistical purposes; and
   - Information covered by legal professional privilege.
Other exemptions are detailed at Annex D.

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

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

10. Preparing the response:
   - When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case by the due date.
   - A copy of the information should be supplied in a permanent form except where the individual agrees or where it is not possible in the format requested or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form. Advice should be taken from the IG team before refusing on these grounds. An alternative would be to allow the individual to view the information. You have 40 calendar days (maximum of one month under GDPR) to comply with the request starting from the date you receive all the information necessary to deal with the request and any fee that is required. It is an offence under the Data Protection Act 1998 (GDPR from 25th May 2018) and individuals can complain to the Information Commissioners Office or apply to a court if you do not respond within this time limit. **NB** Under no circumstances should original records be sent to the applicant.

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

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

‘Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG’s disciplinary procedure’.

7 TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet.

8 MONITORING & AUDIT

1. Performance against the Information Governance Toolkit will be reviewed on an annual basis and used to inform the development of future procedural documents.

2. This standard will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:
   - legislative changes;
   - good practice guidance;
   - case law;
   - significant incidents reported;
   - new vulnerabilities; and
   - changes to organisational infrastructure.

9 REPORTING SECURITY INCIDENTS AND ASSURANCES FROM IT SUPPLIERS

- All information management and technology security (Cyber) incidents and weaknesses must be reported immediately in line with the CCG Incident Reporting Policy.
- Incidents that present an immediate risk to the CCG such as viruses should also be reported to the IT Service Desk immediately.
- Information Security Incidents, especially those involving the loss of sensitive or confidential data, or any incident involving unencrypted portable devices may need to be reported as a Serious Incident and/or to the Information Commissioner via the Information Governance Toolkit reporting system. See the Incident Reporting policy for more details.
- There is a legal requirement to report any such serious incidents to the authorities within 72 hours.
- All staff undertake appropriate annual data security training, renamed "Data Security Awareness Level 1" to reflect Data Security Standard 3 in the Caldicott 3 Review, and pass a mandatory test.
- The CCG obtains regular assurance from Core IT providers that CareCert Alerts are being acted upon and are being addressed appropriately. CareCert informs organisations about cyber security vulnerabilities, mitigating risks, and reacting to cyber security threats and attacks.
POLICY REVIEW

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

Reference Materials

This procedure is in place to ensure the organisation’s compliance with legislation and guidance including, but not limited to, the following:

- The Data Protection Act 1998
- General Data Protection Regulation (GDPR)
- The Health and Social Care Act 2012
- The Human Rights Act 1998
- Caldicott 2 Principles –To Share or Not to Share? The Information Governance Review April 2013
- Common Law Duty of Confidentiality
- NHS Care Records Guarantee for England
- HSCIC Guide to Confidentiality in Health and Social Care
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- The Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Mental Capacity Act 2005
- Records Management Code of Practice for Health and Social Care 2016
- NHS Act 2006
- Public Records Act 1958
Annex A - Registration & Authentication Examples of Documentary Evidence

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

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

**Active in the Community**

“Active in the Community” documents should be recent (at least one should be within the last six months unless there is a good reason why not) and should contain the name and address of the registrant.
- record of home visit
- confirmation from an Electoral Register search that a person of that name lives at that address
- recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed)
- local authority tax bill (valid for current year)
- current UK photo card driving licence (if not used for evidence of name)
- current full UK driving licence (old version) (if not used for evidence of name)
- bank, building society or credit union statement or passbook containing current address
- recent original mortgage statement from a recognised lender
- current local council rent card or tenancy agreement
- current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit
- court order
### Annex B – Subject Access Request Exemptions

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

<table>
<thead>
<tr>
<th>Policy / Project / Function:</th>
<th>Subject Access Request Policy v1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Analysis:</td>
<td>02/11/17</td>
</tr>
<tr>
<td>Completed by:</td>
<td>Dr Mark Culling</td>
</tr>
<tr>
<td>(Name and Department)</td>
<td>eMBED IG Team</td>
</tr>
</tbody>
</table>

**What are the aims and intended effects of this policy, project or function?**

The overall purpose of the policy is to set out the CCG’s approach to Access to Health Records within the workplace. The policy will also set out guidance to staff and managers about their responsibilities in relation to Access to Health Records.

**Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?**

No

**Please list any other policies that are related to or referred to as part of this analysis**

- The Health and Social Care Act 2012
- The Human Rights Act 1998
- Caldicott 2 Principles –To Share or Not to Share? The Information Governance Review April 2013
- Common Law Duty of Confidentiality
- NHS Care Records Guarantee for England
- HSCIC Guide to Confidentiality in Health and Social Care
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- The Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Mental Capacity Act 2005
- Records Management Code of Practice for Health and Social Care 2016
- NHS Act 2006
- Public Records Act 1958
- General Data Protection Regulation (GDPR) (from 25th May 2018)
- Protection Act 1998 (superseded by...
<table>
<thead>
<tr>
<th>Who will the policy, project or function affect?</th>
<th>Employees and the general public</th>
</tr>
</thead>
<tbody>
<tr>
<td>What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?</td>
<td>Consultation on the new policy has taken place nationally and locally. Consultation on the updated policy has taken place locally.</td>
</tr>
</tbody>
</table>

Promoting Inclusivity and Hull CCG’s Equality Objectives.

How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation?

How does the policy promote our equality objectives:

1. Ensure patients and public have improved access to information and minimise communications barriers
2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone’s day-to-day job
3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve
4. Ensure that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs

The policy does not directly promote inclusivity but provides a framework for the handling of access to health records ensuring staff are supported by management and health professionals.
<table>
<thead>
<tr>
<th>Equality Data</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is any Equality Data available relating to the use or implementation of this policy, project or function?</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine Protected Characteristics – referred to hereafter as ‘Equality Groups’.

Examples of Equality Data include: (this list is not definitive)

1. Recruitment data, e.g. applications compared to the population profile, application success rates
2. Complaints by groups who share / represent protected characteristics
3. Grievances or decisions upheld and dismissed by protected characteristic group
4. Insight gained through engagement

Where you have answered yes, please incorporate this data when performing the Equality Impact Assessment Test (the next section of this document).

If you answered No, what information will you use to assess impact?

Please note that due to the small number of staff employed by the CCG, data with returns small enough to identify individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.
## Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?

(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

<table>
<thead>
<tr>
<th>Protected Characteristic:</th>
<th>No Impact:</th>
<th>Positive Impact:</th>
<th>Negative Impact:</th>
<th>Evidence of impact and, if applicable, justification where a <strong>Genuine Determining Reason</strong>(^1) exists (see footnote below – seek further advice in this case)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>X</td>
<td></td>
<td></td>
<td>This policy applies to all regardless of gender</td>
</tr>
<tr>
<td>Age</td>
<td>X</td>
<td></td>
<td></td>
<td>This policy applies to all regardless of age</td>
</tr>
<tr>
<td>Race / ethnicity / nationality</td>
<td>X</td>
<td></td>
<td></td>
<td>This policy applies to all staff regardless of race/ethnicity. Analysis of employee data indicates that the percentage of white employees is reflective of the local population. However, the proportion of BME staff is lower than that of the local population it serves. All staff require competencies which include the ability to read and understand English or to request</td>
</tr>
</tbody>
</table>

---

\(^1\) The action is proportionate to the legitimate aims of the organisation (please seek further advice)
<table>
<thead>
<tr>
<th>Identity Type</th>
<th>X</th>
<th>This policy applies to all regardless of</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disability</td>
<td></td>
<td>disability</td>
<td></td>
</tr>
<tr>
<td>Religion or Belief</td>
<td></td>
<td>religion or belief</td>
<td></td>
</tr>
<tr>
<td>Sexual Orientation</td>
<td></td>
<td>sexual orientation</td>
<td></td>
</tr>
<tr>
<td>Pregnancy and Maternity</td>
<td></td>
<td>pregnancy or maternity</td>
<td></td>
</tr>
<tr>
<td>Transgender / Gender reassignment</td>
<td></td>
<td>transgender/gender reassignment</td>
<td></td>
</tr>
<tr>
<td>Marriage or civil partnership</td>
<td></td>
<td>marriage or civil partnership</td>
<td></td>
</tr>
</tbody>
</table>

**Action Planning:**

As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?

<table>
<thead>
<tr>
<th>Identified Risk:</th>
<th>Recommended Actions:</th>
<th>Responsible Lead:</th>
<th>Completion Date:</th>
<th>Review Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>As the policy is written in English there is a potential impact on employees whose first language is not English and therefore may struggle reading the policy.</td>
<td>The CCGs internal ‘portal’ and external website signpost individuals to alternative formats such as large print, braille or another language.</td>
<td>CCG Communications</td>
<td>Updating of this facility is ongoing</td>
<td>Next Policy Review - November 2019</td>
</tr>
</tbody>
</table>
### Sign-off

All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs

I agree with this assessment / action plan

If disagree, state action/s required, reasons and details of who is to carry them out with timescales:

____________________________

Signed:

Date: 3.11.17