

# ACCESS TO RECORDS POLICY

## August 2019

**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.

**If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email [HULLCCG.contactus@nhs.net](mailto:HULLCCG.contactus@nhs.net), or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.**

|                      |                             |
|----------------------|-----------------------------|
| Name of Policy:      | Access to Records Policy    |
| Date Issued:         | September 2019              |
| Date to be reviewed: | 2 years after approval date |

|   |  |                |
|---|--|----------------|
| <b>Policy Title:</b>                    | Access to Records Policy   |                |
| <b>Supersedes: (Please List)</b>        | Subject Access Request Policy v1.2   |                |
| <b>Description of Amendment(s):</b>     | <p>This policy is based on the previous Subject: Access Request Policies with the following additions</p> <p>Amendments to remove DPA98 – replaced with DPA18 and GDPR</p> <p>Minor changes to Principles</p> <p>Removal of requirement to request SARs in writing.</p> <p>Updates to section 9 - Requests and preparation for access</p> <p>Updates to section 10 – Timescales</p> <p>Updates to Articles in Section 11</p> <p>Updates to Section 14 – Charges</p> <p>Updates to Appendix A – Charges and Timescales</p> <p>Updates to General Notes – Charges &amp; Timescales</p> <p>Restructure of contents page</p> |                |
| <b>This policy will impact on:</b>      | All Staff and relevant others  |                |
| <b>Policy Area:</b>                     | Information Governance   |                |
| <b>Version No:</b>                      | V1.0   |                |
| <b>Author:</b>                          | Hayley Gillingwater, Senior Information Governance Specialist  |                |
| <b>Effective Date:</b>                  | September 2019   |                |
| <b>Review Date:</b>                     | August 2021  |                |
| <b>Equality Impact Assessment Date:</b> | August 2019  |                |
| <b>APPROVAL RECORD</b>                  |  | <b>Date:</b>   |
|   | Integrated Audit and Governance Committee  | September 2019 |
| <b>Consultation:</b>                    | Information Governance Steering Group  | August 2019    |
|   | Senior Leadership Team / Relevant Others   | August 2019    |



## CONTENTS

|                   |  | Page |
|-------------------|--|------|
| 1.                | <b>INTRODUCTION</b>  | 4    |
| 2.                | <b>BACKGROUND</b>  | 4    |
| 3.                | <b>SCOPE</b>   | 5    |
| 4.                | <b>IMPACT ANALYSIS</b><br>Equality   | 5    |
| 5.                | <b>BRIBERY ACT 2010</b>  | 5    |
| 6.                | <b>POLICY PURPOSE AND AIMS</b>   | 6    |
| 7.                | <b>NHS CONSTITUTION</b><br>The CCG is committed to:<br>This Policy supports the NHS Constitution and | 10   |
| 8.                | <b>ROLES / RESPONSIBILITIES / DUTIES</b>   | 10   |
| 9.                | <b>IMPLEMENTATION</b>  | 14   |
| 10.               | <b>TRAINING AND AWARENESS</b>  | 15   |
| 11.               | <b>MONITORING AND EFFECTIVENESS</b>  | 15   |
| 12.               | <b>POLICY REVIEW</b>   | 15   |
| 13.               | <b>REFERENCES</b>  | 15   |
| <b>APPENDICES</b> |  |      |
| Appendix A        | <b>REQUEST FOR ACCESS TO HEALTH RECORDS</b>  | 17   |
| Appendix B        | <b>GUIDANCE FOR APPLICANTS</b>   | 19   |
| Appendix C        | <b>FREQUENTLY ASKED QUESTIONS</b>  | 22   |

## 1. INTRODUCTION

This protocol provides information in relation to the Access to Health Records Act 1990, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), and details the procedures that the 'organisation' has in place to enable patients, service users and staff to access records held about them. Also included, is the protocol for managing access requests from other parties representing the patient, for example, a solicitor.

## 2. BACKGROUND

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR), impose constraints on the processing of personal information in relation to living individuals. The GDPR identifies seven data protection principles that set out standards for information handling. In the context of confidentiality, the most significant principles are:

- Principle 1 which requires processing to be fair and lawful and imposes other restrictions
- Principle 2 which requires personal data to be processed for one or more specified and lawful purpose(s);
- Principle 6 which requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage

Under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), the following people are entitled to request access to individual health records or organisational staff records, regardless of when the record was created:

- the patient;
- another person (on receipt of the patient's consent);
- the parent or guardian for a child under the age of 13

*(where a child is considered capable of making decisions about his/her medical treatment, the consent of the child must be sought before a person with parental responsibility can be given access);*

- A court appointed representative of someone who is not able to manage their own affairs.

### **Access to Health Records of deceased patients**

Under the Access to Health Records Act 1990, when a patient has died, the personal representative, executor or administrator, or anyone having a claim resulting from the death (this could be a relative or another person), may apply to see the health records or part of them.

### 3. **SCOPE**

This policy applies to those members of staff that are directly employed by the Clinical Commissioning Group (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 policy 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.

### 4. **IMPACT ANALYSIS**

#### **Equality**

An equality impact screening analysis has been carried out on this protocol.

As a result of performing the analysis, the protocol does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage; details are available alongside this protocol on the CCG's website.

### 5. **BRIBERY ACT 2010**

Under the Bribery Act 2010, it is a criminal offence:

- To bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so;
- To be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so;
- To bribe a foreign public official – A person will be guilty of this offence if they promise, offer or give a financial or other advantage to a foreign public official, either directly or through a third party, where such an advantage is not legitimately due; and
- If commercial organisations fail to embed preventative bribery measures. This applies to all commercial organisations which have business in the UK. Unlike corporate manslaughter this does not apply to the organisation itself; individuals and employees may also be guilty.

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It is therefore, extremely important that staff adhere to this and other related policies and documentation (as detailed on the CCG's intranet) when considering whether to offer or accept gifts and hospitality and/or other incentives.

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see <http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf>.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or email at [nikki.cooper1@nhs.net](mailto:nikki.cooper1@nhs.net).

Due consideration has been given to the Bribery Act 2010 in the development of this policy review and no specific risks were identified.

## **6. POLICY PURPOSE AND AIMS**

### **EXEMPTIONS**

Certain information may be exempt from disclosure under the terms of the Data Protection Act 2018 and the GDPR and access may therefore be refused should the information be covered by one of the following exemptions:

- To avoid prejudicing the carrying out of professional/clinical work by causing serious harm to the physical or mental health or condition of the data subject or another person.
- Where disclosure would, in the view of a health professional, be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.
- When disclosing the records would reveal information that relates to or identifies another person unless their consent has been given (except where it is reasonable to disclose the records without that person's consent)
- Where other enactments themselves prevent disclosure e.g. adoption records and reports.
- Where an access request has previously been met the Act permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between.

*(See page 9 for further details as to how to apply the above exemptions)*

## **RIGHT OF ACCESS**

Any living person, who is the subject of personal information held and processed by a statutory agency, has a right of access to the data held about them (subject to the limited number of exemptions above).

A person does not have the right to know what is recorded about someone else. For example, where records contain information about a family, one member is not entitled to see information about another member without that person's consent, although there may be circumstances in which it may be considered reasonable to disclose such information without consent (see 7.3). An example would be when a request received for access to very old files and the possibility of establishing the consent of third parties is remote, or non-existent. Each case would be assessed on an individual basis.

### **Requests made on behalf of an adult lacking mental capacity**

If a person lacks the capacity or ability to manage their own affairs, a person acting under an order of the Court of Protection or acting within the terms of a registered Enduring Power of Attorney can request access on her or his behalf. This can be:

- 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

Many people suffering from mental disorder have sufficient capacity to enable them to deal with their affairs. Requests for access by persons with a mental disorder will require a judgement in respect of their capacity to understand the nature of the request and the information sought. This judgement should be made by a health professional. Each case would be assessed on an individual basis.

### **Requests made through another person (an agent)**

If a person has the capacity and they have appointed an agent, that person can make a valid request for access on behalf of the "data subject". Agents should provide evidence of their authority and confirm their identity and relationship to the individual. Such evidence should be:- Photographic evidence i.e. Passport / Full driving licence of the data subject and evidence of activity in the community with evidence of address, i.e. council tax bill, bank statement utility bill (Not mobile phone bill). These should be copied and placed with the application file. If the applicant is acting on behalf of someone else, then a letter of consent from the data subject would be required as well. If using 'Power of attorney' the same documents should be used in respect of the applicant.

Once it is confirmed that the data subject has authorised the agent to make the request, it may be treated as if the request had been made by the person

themselves. If someone is acting on someone else's behalf under a general power of attorney, written authorisation is also required.

A person who is profoundly physically disabled may not be able to give written consent for an agent to seek access on their behalf. Where the person is unable to give written consent, health services should provide appropriate assistance. A qualified health professional will be required to make a judgement on whether the individual has given consent for an agent to act on their behalf.

### **Requests by solicitors etc, regarding criminal injuries, persons**

Requests for access from a person's legal representative must be treated in the same way as requests made by an agent as outlined above.

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

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 office 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.

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

### **Requests for access to the records of a deceased person**

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) applies only to the processing of personal information in relation to living individuals. Information held on the deceased is not personal data, as defined by the Act, and is therefore covered by the Access to Health Records Act 1990. There may still be issues of confidentiality surrounding the rights of others to access the records of a deceased patient and again, each case will be assessed on an individual basis.

This protocol is not intended to support or facilitate open access to the health records of the deceased. Individual(s) requesting access to deceased patient health information should be able to demonstrate a legitimate purpose, generally a strong public interest justification and in many cases a legitimate relationship with the deceased patient. On making a request for information, the requestor should be asked to provide authenticating details to prove their identity and their relationship with the deceased individual. They should also provide a reason for the request and where possible, specify the parts of the deceased health record they require.

## **Parental access to their child's health record**

Normally a person with parental responsibility will have the right to apply for access to their child's health record. However, in exercising this right a health professional should give careful consideration to the duty of confidentiality owed to the child before disclosure is given.

The law regards young people aged 16 or 17 to be adults in respect of their rights confidentiality. Children under the age of 16 who have the capacity (a child can be considered competent under Gillick/Fraser guidelines), and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected. However, good practice dictates that the child should be encouraged to involve parents or other legal guardians in their healthcare. Further guidance is expected in relation to the rights of children under GDPR.

## **Request for access**

Under GDPR requests can be made verbally or in writing. (If the request is in writing this may be by letter, fax, email, or even social media, such as Facebook or twitter). A request can be made to any part of the organisation and does not have to be to a specific person or contact point. 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.

## **INFORMATION ABLE TO BE DISCLOSED**

Unless quantified in the request all of the data held by an organisation in relation to a specific patient/service user request should be disclosed, providing an exemption does not apply or another person has declined to consent to the disclosure of any data identifying them. The term data, includes all formats (written records, computer files, video recordings etc) and covers records held within all of the locations where different parts of the record may be held. The rights of access are also irrespective of when the information was recorded, in relation to a live patient.

## **REFUSING ACCESS BASED ON AN EXEMPTION FROM THE DATA PROTECTION ACT 2018 OR THE GENERAL DATA PROTECTION REGULATION (GDPR)**

Use of the exemptions should be made on an individual case basis and should be the exception rather than the rule. Legal advice should be sought where doubt exists. Refer to Legal Team where doubt exists.

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 or the request should be declined unless the other person has provided written consent for the disclosure.
- 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
- A data subject cannot rely on the DPA 2018 or the GDPR to seek access to records where other enactments themselves prevent disclosure, for example, adoption records and reports; parental order records and reports under Section 30 of the Human Fertilisation and Embryology Act 1990.

## **7. NHS CONSTITUTION**

7.1 The CCG is committed to: Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

7.2 This Policy supports the NHS Constitution as follows:  
The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

## **8. ROLES / RESPONSIBILITIES / DUTIES**

### **Role of the Caldicott Guardian**

The Caldicott Guardian is responsible for acting as a champion for data confidentiality and for developing their knowledge of confidentiality and data protection matters including links with external sources of advice and guidance to allow them to manage this subject area. They should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff and oversee all arrangements, protocols and procedures where

confidential information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

The Caldicott Guardian is responsible for ensuring that NHS and partner organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Caldicott Guardian actively supports work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information as required. Local issues will inevitably arise for Caldicott Guardians to resolve. Many of these will relate to the legal and ethical decisions required to ensure appropriate information sharing. It is essential in these circumstances for Guardians to know when, and where, to seek advice.

A key recommendation is that every use or flow of patient-identifiable information should be regularly justified and routinely tested against the seven defined principles:

Principle 1 – Justify the purpose(s) for using confidential information

Principle 2 – Only use it when absolutely necessary

Principle 3 – use the minimum that is required

Principle 4 – Access should be on a strict need-to-know basis

Principle 5 – Everyone must understand his or her responsibilities

Principle 6 – Understand and comply with the law

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

## **REQUESTS AND PREPARATION FOR ACCESS**

Explain the access procedures to the patient/service user, including an explanation of the time periods and deadlines applicable (see [Appendix B](#) for Guidance Notes for Applicants). An FAQ section can be found in [Appendix C](#).

The data subject can make a request verbally or in writing. For written requests there is an application form available (see [Appendix A](#) Application Form for Processing Subject Access Requests). The data subject is **NOT** required to use this application form, a request in any format is acceptable and must be handled accordingly.

Ensure the subject submits sufficient details to identify themselves, and that there is a clear indication as to the information requested and where it may be held (i.e. treatment locations). This will ensure the request can be processed and managed successfully and efficiently.

Should an exemption apply, the data-controller should agree with their manager, and in consultation with the relevant health care professional, exactly what information cannot be shared with the patient/service user. The subject should then

be contacted as soon as possible to inform them of the decision, and this should be supported in writing detailing the reasons for the decision at the earliest opportunity.

Written consent must be obtained from all third parties who have contributed to the record, if that information is to be shared with the subject. If consent cannot be obtained, is refused, or requires a disproportionate effort to obtain, information relating to third parties should be redacted.

## **TIMESCALES**

### **It is important to note that:**

If the person has been receiving treatment during the preceding one month no more than 21 calendar days must elapse between receiving the request for access (which must include the consent to release were applicable) and the records being released.

If treatment was last given over one month ago then no more than one month must elapse after the application has been made before access is given.

The 21 days and one month periods do not start until the request has been received in full and the identity or authority of the person making the request can be validated. In exceptional circumstances these timescales can be extended by mutual agreement of both parties.

Consents from third parties should be sought to fit within this one month timescale.

Access can be refused where the authority has previously complied with an identical or similar request from the same individual, unless a reasonable interval has elapsed between compliance with the initial request and the receipt of a further request.

## **CIRCUMSTANCES OF ACCESS**

A copy of the information should be produced for the patient/service user. If the original documents are required then access should be provided to the patient/service user in the presence of the data controller or appropriate clinician.

- 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.

The person may find it helpful to be accompanied by a friend or relative. Separate access must not be given to a friend or relative unless they are the person's appointed agent.

Under no circumstances can any information be removed from the record, although a request for amendments can be submitted where required.

Patients may also apply to NHS organisations for the correction or deletion of their information under Articles 15 and 16 of the General Data Protection Regulation, however, restrictions do apply. NHS bodies should respond within one calendar month to such requests, confirming compliance, or non-compliance and reasons which they believe the request is unjustified.

Anyone making a Subject Access Request 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 an objection to the processing altogether.

## **FORMAT**

The person is entitled to have a permanent copy of the information, unless:

- The person agrees otherwise, for example only having photo-copies of relevant extracts or documents taken from the complete record; or
- It is not possible, or would involve disproportionate effort.

## **ACCESSIBILITY**

People who are unable to read or have a physical disability may have a friend, relative or advocate present at the access interview who can read the record to them.

## **CHARGES**

Under GDPR information must be provided free of charge to applicants. 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 Commissioners Office as soon as possible and at the latest within one month.

**Any charges for access requests should not be made in order to make a financial gain.**

Requests should be dealt with within a maximum of 1 calendar month 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 month.

**Note:** if a person wishes to view their health records and then wants to be provided with copies this would still come under the one access request.

## **AMENDMENTS/CORRECTIONS**

A patient/service user is entitled to ask the agency to correct data if the personal information is inaccurate in any way i.e. it is factually incorrect or misleading. They are not entitled to alter clinical judgements, diagnosis etc.

The person must be informed within 21 days of receiving the request of any action that is to be taken in response to their request to correct inaccurate data.

If there is an administrative error within the record and both the subject and the data-controller agree, a correction can be made. A copy of the corrected data should be given to the subject.

Where there is a disagreement about the accuracy of a record, the subject should have his/her account of the situation added and the fact of the disagreement recorded. The person can:

- Approach the Information Commissioners Office (ICO) if they consider the organisation has not made the requested correction;
- Apply to the courts for an order requiring the organisation to rectify, block, erase or destroy the data.

The organisation may be required to correct the data if the IC or courts judge it to be inaccurate, and to inform other organisations who may have reviewed the information of the correction.

## **ACCESS TO VIDEO AND AUDIO RECORDINGS**

The same rules apply to access to video and audio recording as to other types of record.

If a patient/service user is to be recorded or videoed, the procedure for handling and deleting the recording must be explained to them beforehand.

If a video/audio recording has been deleted the patient/service user must be shown the entry in the case record which must state the date and reason for deletion.

## **9. IMPLEMENTATION**

The policy will be disseminated by being made available on the website 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'.*

## **10. TRAINING AND AWARENESS**

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

## **11. MONITORING AND EFFECTIVENESS**

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

This standard will be reviewed on an annual basis, and in accordance with the on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

## **10. 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.

## **11. REFERENCES**

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 2018
- 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

## APPENDICES

### APPENDIX A

#### REQUEST FOR ACCESS TO HEALTH RECORDS

##### DETAILS OF THE RECORD TO BE ACCESSED

**Patient** Surname .....

Forename(s) .....

Date of Birth ..... / ..... / ..... NHS Number (*if known*) .....

Hospital Reference Number (*if known*) .....

Please indicate which records you require to enable us to locate the information within the specified timescale.

.....  
**Details of Applicant (if different from above)**

**Applicant's** Surname .....

Forename(s).....

##### DECLARATION

I declare that information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record referred to above, under the terms of the Access to Health Records Act (1990) / Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

- I am the patient
- I have been asked to act by the patient and attach the patient's written authorisation.
- I have parental responsibility/legal guardianship for the patient who is under age 16 and [is incapable of understanding the request][has consented to me making this request] (delete appropriately)
- I have been appointed the Guardian for the patient, who is over age 16 under a Guardianship order
- I am the deceased patient's personal representative and attach confirmation of my appointment.
- I have a claim arising from the patient's death and wish to access information relevant to my claim on grounds that:

.....  
.....  
I am aware that information must be provided free of charge unless my request is manifestly unfounded or excessive, in which case the CCG may charge a fee based on the administration costs of the request.

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

**Please Note: It will be necessary to provide evidence of identity (i.e.: Driving Licence). If there is any doubt of the applicant's identity or entitlement, information may not be released. You will be informed if this is the case. (See guidance for applicants proof of identity in Appendix C)**

**Official Use Only:**

**Pre-processing check**

- Sufficient details to process application [date] ..... / ..... / ..... Signed: .....
- 'NO': Letter sent to seek further information [date]: ..... / ..... / ..... Signed: .....
- Proceed

**NOTE: INFORMATION MUST BE PROVIDED WITHIN A MAXIMUM OF ONE MONTH OF RECEIPT OF THE COMPLETED APPLICATION.**

**Processing of request**

Name of Lead Health Professional: .....

- Correspondence sent / contacted [date]:..... Signed: .....
- Outcome:  Appointment to be made with Lead Health Professional  
made for [date]: ..... at [time]: ..... Initials: .....
- Supervised Appointment to be made with: .....  
made for [date]: ..... at [time]: ..... Initials: .....
- Copies of notes to be sent
- Applicant advised of outcome [date]: ..... Signed: .....

**Processing Application:**

Access provided on [date] ..... / ..... / .....

Further Action: Corrections requested Yes / No

Copies provided Yes / No Copying fee (£.....) Yes / No

Comments:

Fees for additional copies of information already provided:

Copy of notes:  made [date] ..... / ..... / ..... Signed: .....

Copying fee: £ ..... P & P: £ ..... Total: £.....

sent [date] ..... / ..... / ..... Signed: .....

Finance Advised [date] ..... / ..... / ..... Signed: .....

Fee received [date] ..... / ..... / ..... Signed: .....

## APPENDIX B

### GUIDANCE FOR APPLICANTS

#### REQUEST FOR ACCESS TO HEALTH RECORDS

#### GUIDANCE NOTES FOR APPLICANTS

##### Introduction

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) provides individuals with the right to access personal information held about them. Under the Subject Access procedure you, as an individual, are entitled to:

- Be informed whether personal information is held about you;
- Be supplied with a copy of that information, a description of the purpose(s) for which the information has been processed and to whom has access to the information;
- Be supplied with a description of the data and its sources(s), and
- Know the logic involved in any decision-making affecting the individual where the data forms the basis for that decision.

##### Who can access a record?

- The patient;
- Another person (with the patient's written permission);
- A parent or a guardian of a person under 16. (Where a child is considered capable of making decisions about his/her treatment, the consent of the child must be sought before a person with parental responsibility can be given access);
- A court appointed representative of someone who is not able to manage their own affairs;
- Where the patient has died, the personal representative or executor or administrator or anyone having a claim resulting from the death (this could be a relative or another person), may apply to see the records, or part of them.

### **When can the record holder refuse to provide the information?**

Under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) you have a right to see information held about you subject to certain safeguards (exemptions):

- When the record holder thinks access is likely to cause you or anyone else serious physical and mental harm;
- When the record contains details that the patient has asked not to be revealed to a third party;
- When disclosing the records would reveal information that relates to or identifies another person unless their consent has been given (except where it is reasonable to disclose the records without that person's consent);
- When the records have been destroyed under Records Management NHS Code of Practice.

### **Proof of identity**

If you are applying for your own records please send a copy of one of the following:

- Passport
- Photo card Driving License
- Birth Certificate

Please DO NOT send the original documents.

If you are applying for records on behalf of a patient you will need to provide proof of your identity (as above) and you must also include the patient's written authorisation for you to have access to their records.

If you are applying for the records of a deceased individual you must include proof of your own identity together with proof of a court appointment as personal representative.

### **Type of records required**

It is important that you provide us with as much information as possible regarding the records you wish to have access to and the time period for which you are referring to.

## GENERAL NOTES

### **Fees:**

Information must be provided free of charge under GDPR unless the request is manifestly unfounded or excessive.

Your completed application form (should you choose to use our template) and identification should be forwarded to:

Corporate Governance Team  
Hull CCG  
2<sup>nd</sup> Floor Wilberforce Court  
Alfred Gelder Street  
Hull  
HU1 1UY

Alternatively you can contact the CCG at: [HULLCCG.contactus@nhs.net](mailto:HULLCCG.contactus@nhs.net) / 01482 344700

### **How long will it take to process my application?**

We aim to ensure you have access to your records within a maximum of one month of receiving your request and proof of your identity. If the person has been receiving treatment within the preceding one month then we will aim to release the records within 21 days. In exceptional circumstances it may be necessary to exceed these deadlines, however you will be informed accordingly should this prove to be the case.

In some cases, a clinician may invite you to attend a “counselling” meeting in order to explain the meaning of the data we hold about you. You are not obliged to accept such an invitation unless you wish to do so but it would be in your best interests to accept. If, on the receipt of any data, you wish to seek further clarification, challenge the accuracy of the data or require further advice about your rights under the Data Protection Act 2018 or the General Data Protection Regulation (GDPR), please contact, in writing, the Primary Care Trust in the first instance.

## APPENDIX C

### Frequently Asked Questions

**Q. Do I have to use an Act to apply for access to my health information?**

A. Although Acts such as the DPA, GDPR and AHRA provide a statutory right of access to information; NHS organisations can choose to disclose information to individuals outside of the provisions of these Acts, subject to confidentiality considerations.

**Q. Can information about third parties be disclosed within a health record?**

A. Careful consideration should be made before disclosing third party information, and consent should normally be sought before disclosure. Where it can be demonstrated that consent is not practicable, the NHS organisation should weigh up whether the third party information should be fully released or removed. All disclosures of information about third parties need to be considered on a case-by-case basis, and decisions about disclosure should be fully documented.

**Q. Can information within a health record which identifies health professionals be disclosed to a patient?**

A. Information about health professionals is not normally considered as 'third party' information, and as such should normally be disclosed as part of a request unless disclosure would put any person at risk of harm.

**Q. Should individuals be informed if information is withheld from a request?**

A. NHS bodies should normally inform patients if information is withheld from them during an access request unless doing so would put any person at risk, or would disclose information or inappropriately identify a third party.

**Q. Do researchers have a right to access information from patient health records when they are unable to gain patient consent?**

A. Research using health information can provide many potential benefits. Researchers wishing to access information should follow NHS Research Governance processes and in most cases where access to identifiable information is sought they should obtain approval from the Ethics and Confidentiality Committee of the statutory National Information Governance Advisory Board.

**Q. Can MPs have access to health information about their constituents?**

A. The term 'elected representative' covers Members of Parliament (UK, Scotland, Wales, Northern Ireland and EU), local authority councillors and mayors (and their equivalents in the devolved countries). Specific legislation under the Statutory Instrument, 2002, No. 2905, The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 enables information to be disclosed to elected representatives without contravening the Data Protection Act 2018 or the General Data Protection Regulation (GDPR). However, it does not remove the constraints of the common law duty of confidentiality and as such the common law should still be satisfied (normally by consent) before information is disclosed.<sup>1</sup>

**Q. Should all information available be disclosed to a LSCB when investigating a child's death?**

A. Local Safeguarding Children's Boards may require access to health records relevant to a deceased child from an NHS body to conduct an investigation/inquiry. It is highly likely that the public interest served by this process warrants full disclosure of all relevant information within the child's own records. However, in some circumstances the LSCB may also require access to information about third parties (e.g. members of the child's immediate family or carers). In all cases the LSCB should explain why it believes information about third parties is relevant to its enquiries, and you should use this to consider whether or not there is an overriding public interest to justify the disclosure of the information requested. In cases where you determine disclosure to be in the public interest you must ensure that any information you disclose about a third party is both necessary and proportionate.

**Q. Should all information requested be disclosed to Coroners for the purpose of carrying out an inquiry?<sup>2</sup>**

A. It is the Department of Health's view that the public interest served by Coroners' inquiries will outweigh considerations of confidentiality unless exceptional circumstances apply.

When an NHS organisation feels that there are reasons why full disclosure is not appropriate, e.g. due to confidentiality obligations or Human Rights considerations, the following steps should be taken:

- a) the Coroner should be informed about the existence of information relevant to an inquiry in all cases;
- b) the concern about disclosure should be discussed with the Coroner and attempts made to reach agreement on the confidential handling of records or partial redaction of record content;
- c) where agreement cannot be reached the issue will need to be considered by an administrative court.

<sup>1</sup> Section 13 of Model B3 in Confidentiality: NHS Code of Practice (DH 2003) provides more information about disclosures to MPs

<sup>2</sup> Coroners' inquiries are an important part of determining cause of death in a huge number of cases in the UK. Prompt access to confidential information regarding patients and others involved in an investigation is often vital to the reliability of the outcome of an inquiry.

**Q. Should consideration be given to surviving family members when disclosing information about deceased patients?**

A. NHS body's should have consideration to the potential harm or distress to the requester or other individuals either through supplying or withholding information. Where information is disclosed the amount of information provided should be proportionate to the need. Requesters should be sensitively informed where the decision is taken to withhold information.

**Q. How do Independent Mental Health Advocates (IMHAs) and The Mental Health Act 1983 apply to access to health records?**

A. Under this Act, certain people (“qualifying patients”) are entitled to support from an IMHA subject to certain conditions, section 130B of that Act says that, for the purpose of providing help to a qualifying patient, IMHAs may require the production of and inspect any records relating to the patient’s detention or treatment in any hospital or to any after-care services provided for the patient under section 117 of the Act.<sup>3</sup>

The Department has published guidance on IMHAs’ rights to information which would not be disclosed in response to an access request from the qualifying patient themselves. This is available on the Department of Health website:

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_098828](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_098828)

**Q. How do Deputies and Lasting Powers of Attorney and The Mental Capacity Act 2005 (MCA) apply to access to health records?**

A. The MCA generally only affects people aged 16 or over. The Act provides a statutory framework to empower and protect people who may lack capacity to make some decisions. The MCA set up a new Court of Protection, which is permitted to appoint a deputy, to deal with property and affairs and/or personal welfare decisions. People whilst they still have capacity can appoint a Lasting Power of Attorney, also either for property and affairs and / or personal welfare decisions. Personal welfare deputies and attorneys can ask to see information concerning the person they are representing as long as the information applies to decisions they have the legal right to make.<sup>4</sup>

<sup>3</sup> Chapter 20 of the Code of Practice: Mental Health Act 1983 provides more information: [www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_084597](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_084597)

<sup>4</sup> The Department of Health, in partnership with the Welsh Assembly Government and the Social Care Institute for Excellence, has published a range of materials including training materials to support the implementation of the MCA that can be downloaded from the DH website:

<http://www.dh.gov.uk/en/SocialCare/Deliveringadultsocialcare/MentalCapacity/MentalCapacityAct2005/index.htm>

**Q. Can NHS bodies disclose information in response to allegations made about the operation and conduct of its staff?**

A. Where allegations are made against a NHS body in the media by patients or relatives the NHS body may wish to respond in order to maintain the reputation of the NHS. However, in doing so, NHS body should not disclose further confidential information and the level of disclosure should be proportionate to the need, with strong considerations on the impact of possible harm caused to others.

**Q. How long should health records be kept for?**

A. NHS organisations should retain records in accordance with the retention schedules outlined in the Department of Health Records Management NHS Code of Practice before determining whether they should be archived or destroyed<sup>5</sup>. Where records are to be archived they should be transferred to a designated local Place of Deposit (POD) or to the National Archives. The Code is available from the following link:

<http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Recordsmanagement/index.htm>

**Q. What if records are stored at an archive?**

A. Archives may also receive requests for deceased health information from individuals and may consider the use of this guidance as a framework on decisions for disclosure.

<sup>5</sup> The Department of Health's Records Management: NHS Code of Practice provides best practice guidance on records management issues and includes a retention schedule for various categories of records.

| HR / Corporate Policy Equality Impact Analysis:   |   |
|---|---|
| <b>Policy / Project / Function:</b>   | Access to Records Procedure V1.2  |
| <b>Date of Analysis:</b>  | 07/08/2019  |
| <b>Completed by:<br/>(Name and Department)</b>  | Hayley Gillingwater, Senior Information Governance Specialist eMBED IG Team   |
| <b>What are the aims and intended effects of this policy, project or function?</b>  | 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.  |
| <b>Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?</b> | No  |
| <b>Please list any other policies that are related to or referred to as part of this analysis</b>                         | The Health and Social Care Act 2012<br>The Human Rights Act 1998<br>Caldicott 2 Principles – To Share or Not to Share?<br>The Information Governance Review April 2013<br>Common Law Duty of Confidentiality<br>NHS Care Records Guarantee for England<br>HSCIC Guide to Confidentiality in Health and Social Care<br>Access to Health Records Act 1990<br>Freedom of Information Act 2000<br>The Children Act 2004<br>Safeguarding Vulnerable Groups Act 2006<br>Mental Capacity Act 2005<br>Records Management Code of Practice for Health and Social Care 2016<br>NHS Act 2006<br>Public Records Act 1958<br>General Data Protection Regulation (GDPR)<br>Data Protection Act 2018<br>This list is not exhaustive. |

|   |   |
|---|---|
| <b>Who will the policy, project or function affect?</b>   | Employees and the general public  |
| <b>What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?</b>  | Consultation will take place with Information Governance staff at the Information Governance Steering Group, Senior Leadership Team and relevant others   |
| <p><b>Promoting Inclusivity and Hull CCG's Equality Objectives.</b></p> <p>How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation?</p> <p>How does the policy promote our equality objectives:</p> <ol style="list-style-type: none"> <li>1. Ensure patients and public have improved access to information and minimise communications barriers</li> <li>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</li> <li>3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve</li> <li>4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs</li> </ol> | <p>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</p> |

| <b>Equality Data</b>  |   |
|---|---|
| <p><b>Is any Equality Data available relating to the use or implementation of this policy, project or function?</b></p> <p>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 <i>Protected Characteristics</i> – referred to hereafter as '<i>Equality Groups</i>'.</p> | <p>Yes <input data-bbox="1225 1686 1324 1758" type="checkbox" value="Y"/></p> <p>No <input data-bbox="1225 1792 1324 1863" type="checkbox"/></p> <p>Where you have answered yes, please incorporate this data when performing the <i>Equality Impact Assessment Test</i> (the next section of this document). If you answered No, what information will you use to assess impact?</p> |

|  |   |
|--|---|
| <p>Examples of <i>Equality Data</i> include: (this list is not definitive)</p> <p>1: Recruitment data, e.g. applications compared to the population profile, application success rates</p> <p>2: Complaints by groups who share / represent protected characteristics</p> <p>4: Grievances or decisions upheld and dismissed by protected characteristic group</p> <p>5: Insight gained through engagement</p> | <p><b>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.</b></p> |
|--|---|

### 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)**

| Protected Characteristic: | No Impact: | Positive Impact: | Negative Impact: | Evidence of impact and, if applicable, justification where a <i>Genuine Determining Reason</i> <sup>1</sup> exists (see footnote below – seek further advice in this case) |
|---------------------------|------------|------------------|------------------|--|
|---------------------------|------------|------------------|------------------|--|

**It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.**

|                                       |   |  |  |   |
|---------------------------------------|---|--|--|---|
| <b>Gender</b>                         | x |  |  | This policy applies to all regardless of gender   |
| <b>Age</b>                            | x |  |  | This policy applies to all regardless of age  |
| <b>Race / ethnicity / nationality</b> | X |  |  | 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 |

1. <sup>1</sup> *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

|  |   |  |  |  |
|--|---|--|--|--|
|  |   |  |  | proportion of BME staff is lower than that of the local population it serves<br>All staff require competencies which include the ability to read and understand English or to request the information in another format available to them. |
| <b>Disability</b>                        | x |  |  | This policy applies to all regardless of disability  |
| <b>Religion or Belief</b>                | x |  |  | This policy applies to all regardless of religion or belief  |
| <b>Sexual Orientation</b>                | x |  |  | This policy applies to all, regardless of sexual orientation   |
| <b>Pregnancy and Maternity</b>           | x |  |  | This policy applies to all regardless of pregnancy or maternity  |
| <b>Transgender / Gender reassignment</b> | x |  |  | This policy applies to all regardless of transgender/gender reassignment   |
| <b>Marriage or civil partnership</b>     | x |  |  | This policy applies to all regardless of marriage or civil partnership   |

### **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?**

| <b>Identified Risk:</b>   | <b>Recommended Actions:</b>   | <b>Responsible Lead:</b> | <b>Completion Date:</b>              | <b>Review Date:</b>         |
|---|---|--------------------------|--------------------------------------|-----------------------------|
| 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. | The CCGs internal 'portal' and external website signpost individuals to alternative formats such as large print, braille or another language. | CCG Communications       | Updating of this facility is ongoing | 2 years from approval date. |

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |
|--|--|
| <b>Sign-off</b>  |  |
| <b>All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs</b>              |  |
| I agree with this assessment / action plan   |  |
| If <i>disagree</i> , state action/s required, reasons and details of who is to carry them out with timescales: |  |
|                              |  |
| Signed:  |  |
| Date: 23.08.19   |  |