Subject Access Request Policy

[Subject Access Rights]
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 INTRODUCTION</td>
<td>4</td>
</tr>
<tr>
<td>2 PURPOSE</td>
<td>4</td>
</tr>
<tr>
<td>3 SCOPE</td>
<td>4</td>
</tr>
<tr>
<td>4 RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES</td>
<td>4</td>
</tr>
<tr>
<td>5 PROCEDURE/IMPLEMENTATION</td>
<td>6</td>
</tr>
<tr>
<td>5.1 The Data Protection Act 2018/The General Data Protection Regulations 2016 (Living Persons)</td>
<td>6</td>
</tr>
<tr>
<td>5.1.1 Data Protection and Access to Health Records</td>
<td>6</td>
</tr>
<tr>
<td>5.1.2 Policy Statement</td>
<td>6</td>
</tr>
<tr>
<td>5.1.3 Right of Access by the Data Subject</td>
<td>6</td>
</tr>
<tr>
<td>5.1.4 Rights of the Data Subject</td>
<td>7</td>
</tr>
<tr>
<td>5.1.5 Appropriate Health Professional</td>
<td>8</td>
</tr>
<tr>
<td>5.1.6 Information Limited or Denied</td>
<td>8</td>
</tr>
<tr>
<td>5.1.7 Patients Living Abroad</td>
<td>9</td>
</tr>
<tr>
<td>5.1.8 Children</td>
<td>9</td>
</tr>
<tr>
<td>5.1.8.1 Parental Responsibility</td>
<td>9</td>
</tr>
<tr>
<td>5.1.8.2 Children and the Internet</td>
<td>10</td>
</tr>
<tr>
<td>5.1.8.3 Subject Access by a Minor</td>
<td>10</td>
</tr>
<tr>
<td>5.1.8.4 Children aged 16 and 17</td>
<td>11</td>
</tr>
<tr>
<td>5.1.8.5 Younger Children</td>
<td>11</td>
</tr>
<tr>
<td>5.1.8.6 Young Persons – Aged 18</td>
<td>11</td>
</tr>
<tr>
<td>5.1.8.7 Children with Learning Disabilities</td>
<td>11</td>
</tr>
<tr>
<td>5.1.9 Requests from other NHS Trusts</td>
<td>11</td>
</tr>
<tr>
<td>5.1.10 Police Requests/Court Orders</td>
<td>12</td>
</tr>
<tr>
<td>5.1.11 War Pensions/Benefits Agency</td>
<td>13</td>
</tr>
<tr>
<td>5.1.12 Litigation against the Trust</td>
<td>13</td>
</tr>
<tr>
<td>5.1.13 Safeguarding Cases</td>
<td>13</td>
</tr>
<tr>
<td>5.1.14 Requests made on behalf of those who lack mental capacity</td>
<td>14</td>
</tr>
<tr>
<td>5.1.15 Process for Dealing with requests</td>
<td>14</td>
</tr>
<tr>
<td>5.2 Access to Health Records Act 1990 (Deceased Persons)</td>
<td>16</td>
</tr>
<tr>
<td>5.2.1 Rights of Access</td>
<td>16</td>
</tr>
<tr>
<td>5.3 Coroner's Requests</td>
<td>16</td>
</tr>
<tr>
<td>5.4 Medical Reports Act 1988</td>
<td>17</td>
</tr>
<tr>
<td>5.5 Freedom of Information Act 2000 and Access to Health Records</td>
<td>17</td>
</tr>
<tr>
<td>5.6 Dealing with Complaints</td>
<td>17</td>
</tr>
</tbody>
</table>
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page No</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 TRAINING IMPLICATIONS</td>
<td>18</td>
</tr>
<tr>
<td>7 MONITORING ARRANGEMENTS</td>
<td>18</td>
</tr>
<tr>
<td>8 EQUALITY IMPACT ASSESSMENT SCREENING</td>
<td>18</td>
</tr>
<tr>
<td>8.1 Privacy, Dignity and Respect</td>
<td>19</td>
</tr>
<tr>
<td>8.2 Mental Capacity Act</td>
<td>19</td>
</tr>
<tr>
<td>9 LINKS TO ANY ASSOCIATED DOCUMENTS</td>
<td>19</td>
</tr>
<tr>
<td>10 REFERENCES</td>
<td>19</td>
</tr>
<tr>
<td>11 APPENDICES</td>
<td>20</td>
</tr>
<tr>
<td>Appx 1 Definitions</td>
<td>21</td>
</tr>
<tr>
<td>Appx 2(i) Application form for Access to Health Records</td>
<td>22</td>
</tr>
<tr>
<td>Appx 2(ii) Application form for Access to Staff Records</td>
<td>24</td>
</tr>
<tr>
<td>Appx 3 3rd party Application form for Health Records</td>
<td>26</td>
</tr>
<tr>
<td>Appx 4 Access to Health Records Leaflet</td>
<td>27</td>
</tr>
<tr>
<td>Appx 5 Redaction Guide</td>
<td>29</td>
</tr>
<tr>
<td>Appx 6(i) Consent to Release Form relating to Health Records</td>
<td>32</td>
</tr>
<tr>
<td>Appx 6(ii) Consent to Release Form relating to Staff Records</td>
<td>33</td>
</tr>
<tr>
<td>Appx 7 Flow Chart and notes – Subject Access Requests received by IG Team</td>
<td>34</td>
</tr>
<tr>
<td>Appx 8 Flow Chart and notes – Subject Access Requests received by Service</td>
<td>36</td>
</tr>
<tr>
<td>Appx 9 Flow Chart and notes – Subject Access Request – Actions</td>
<td>38</td>
</tr>
</tbody>
</table>
1. **INTRODUCTION**

Individuals have a right to apply for access to health information held about them and, in some cases, information held about other people. NHS organisations must ensure they have adequate procedures in place to enable people to exercise this right. This also applies to staff members who wish to access their staff records.

The following guidance (unless otherwise stated) is based on the current Department of Health's Guidance for Access to Health Records Requests [See Section 10], which assists NHS organisations in England through the process of dealing with an access request in accordance with the relevant legislation and any subsequent considerations.

The main legislative measures that give rights of access to health records include:

- **The Data Protection Act 2018 (DPA)/The General Data Protection Regulations 2016 (GDPR)** - rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual’s behalf;

- **The Access to Health Records Act (AHRA) 1990** - rights of access to deceased patients’ health records by specified persons;

- **The Medical Reports Act (MRA) 1988** - rights for individuals to have access to reports, relating to them, provided by medical practitioners for employment or insurance purposes.

2. **PURPOSE**

This document has been written to ensure that all Trust staff comply with the relevant legislation in relation to the provision of a Trust-wide, robust access to health records request service, delivered in partnership with the Information Governance (IG) Team.

The policy provides guidance on the procedure and responsibilities to assist all staff in handling and processing such requests for information.

3. **SCOPE**

This policy applies to all staff working within the Trust, whether employed by the Trust or not; who are involved in handling patient, service user and staff personal information.

4. **RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES**

Persons with lead responsibility for this policy are:
Chief Executive
The Chief Executive has overall accountability for ensuring that all laws are implemented within the Trust including the DPA 2018/GDPR 2016, the AHRA 1990 and the MRA 1988. In addition, the Chief Executive has overall accountability for implementing records management within the Trust.

Senior Information Risk Owner (SIRO)
The SIRO (Director of Health Informatics) is accountable for information risk throughout the organisation.

Caldicott Guardian
The Caldicott Guardian (Medical Director) is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

Data Protection Officer (DPO)
The DPO will assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Information Asset Owners (IAOs)
IAOs are responsible for information assets which include health records within each service. It is the IAO’s responsibility to make sure that staff within Service areas follow the outlined procedures to ensure the Trust is compliant with appropriate laws.

IG Team
The Team is responsible for the administration of a centralised access to health records service ensuring that:
- All requests are appropriate and the consent and identity of the applicant is verified;
- Communications are sent to the applicant throughout the life of the request, from its receipt until the release of the information;
- Requests are recorded and processed in a legally compliant and confidential manner;
- The lead health professionals adhere to the strict timescales laid down by the relevant legislation;
- Potential problems are escalated back to the Service area to reduce the risk of failing to comply with the law;
- Advice is sought where appropriate from health professionals, the Caldicott Guardian, the IG Manager and other members of the IG Team;
- Consent forms and associated documentation are held securely and confidentially and will be retained in line with the Trust's records retention policies as specified in the Corporate Records Policy and the Healthcare Record Keeping Policy;
Advice and guidance are given to all staff in the Trust on the access to records procedure;

5. PROCEDURE/IMPLEMENTATION

5.1 The Data Protection Act 2018/The General Data Protection Regulations 2016

5.1.1 Data Protection and Access to Health Records

The Data Protection Act 2018 (DPA) [Article 15] states that a data subject has the right to obtain from the Trust confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

A health record is defined as a record consisting of information about the physical or mental health or condition of an identifiable individual. This record is made by or on behalf of a health professional in connection with the treatment and care of that individual.

A health record can be recorded in computerised or manual form or in a mixture of both. It may include such things as hand-written clinical notes, letters to and from other health professionals, laboratory reports, radiographs and other imaging records, printouts from monitoring equipment, photographs, videos and tape-recordings of telephone conversations.

Data protection legislation is not confined to health records held for National Health Service purposes: it applies equally to all relevant records relating to living individuals, which includes the private health sector and health professionals’ private practice records.

5.1.2 Policy Statement

5.1.3 Right of Access by the Data Subject

The Data Protection Act 2018 (DPA) [Article 15] states that a data subject has the right to obtain from the Trust confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling [Article 22(1) and (4) DPA] and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Trust shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Trust may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form, for example, pdf. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

5.1.4 Rights of the Data Subject

The Trust shall take appropriate measures to provide any information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Trust shall provide information without undue delay and in any event within one ‘month’ of receipt of the request. The Trust has adopted the ICO’s view of a 28-day period to ensure compliance is always within a calendar month. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Trust shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Information shall be provided free of charge. Where requests from a data
subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Trust may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b) refuse to act on the request.

The Trust shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Where the Trust has reasonable doubts concerning the identity of the individual making the request, it may request the provision of additional information necessary to confirm the identity of the data subject.

Data Protection legislation is not confined to health records held for NHS purposes, it applies to all records relating to living individuals. [See Section 10]

5.1.5 Appropriate Health Professional to Consent to Release

Schedule 3 of the DPA 2018 makes provision for restrictions from certain GDPR provisions where this is necessary for health, education and social work purposes, and defines the appropriate health professional as:

(a) someone who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matters to which the data relates,
(b) where there is more than one such health professional, the one who is the most suitable to provide an opinion on the question, or
(c) the one who has the necessary experience and qualifications to provide an opinion on the question, where:
   (i) there is no health professional available.

5.1.6 Situations Where Health Information May be Limited or Denied

- disclosure of information relating to, or provided by, a third person who has not consented to that disclosure unless:
  - The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient.
  - The third party, who is not a health professional, gives their consent to the disclosure of that information.
  - It is reasonable to disclose without that third party’s consent.

Schedule 3 of the DPA 2018 also enables the data controller to limit or deny access to an individual’s health records where:

- the data would be likely to cause serious harm to the physical or
mental health of the data subject or another individual [Part2(2)]'.—, or

- The granting of access to a patient representative would disclose information which:
  (a) was provided by the data subject in the expectation that it would not be disclosed to the person making the request,
  (b) was obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or
  (b) the data subject has expressly indicated should not be so disclosed.

The above does not apply if:

- the data subject has expressly indicated that they no longer have the expectation.
- The data concerning health has already been seen by, or is within the knowledge of, the data subject.

5.1.7 Patients living abroad requiring access to their health records

Former patients living outside of the UK who had treatment in the UK have the same rights under the DPA to apply for access to their UK health records. An NHS organisation should treat these requests the same as someone making an access request from within the UK.

Original health records must not be given to patients to keep/take to a new health professional outside the UK.

5.1.8 Children’s Information

- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual’s right to erasure is particularly relevant if they gave their consent to processing when they were a child. [ICO Guide to GDPR 2016]

5.1.8.1 Parental access to children’s health records

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 must 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 to confidentiality. Children under the age of 16 who have the capacity 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.

What is parental responsibility?

While the law does not define in detail what parental responsibility is, the following list sets out the key roles for consideration:

- providing a home for the child
- having contact with and living with the child
- protecting and maintaining the child
- disciplining the child
- choosing and providing for the child’s education
- determining the religion of the child
- agreeing to the child’s medical treatment
- naming the child and agreeing to any change of the child’s name
- accompanying the child outside the UK and agreeing to the child’s emigration, should the issue arise
- being responsible for the child’s property
- appointing a guardian for the child, if necessary
- allowing confidential information about the child to be disclosed

You must make reasonable efforts to verify that the person giving consent does, in fact, hold parental responsibility for the child (aged under 18) [DPA 2018 Sched 3 Part 2 4(a)].

5.1.8.2 Children and the Internet (Information Society Services)

Article 8 of The GDPR addresses the issue of whether parental consent is required only in the context of online services. When offering an online service directly to a child, in the UK only children aged 13 or over are able to provide their own consent. Parental consent is required where such services are offered to a child below the age of 13.

Publically funded health and social care online services such as Patient Online are not captured by GDPR because they are (i) not provided for remuneration as the definition of information society services requires and (ii) GDPR only applies where the condition for lawful processing under Article 6 is consent. Furthermore, the GDPR provides interpretation that parental consent ‘...should not be necessary in the context of preventative or counselling services offered directly to a child.’ The Trust’s lawful basis for the provision of publically funded online services is for direct care.

5.1.8.3 Subject Access by a Minor

[also see 5.1.8] The right of access by a minor must be assessed by application of the same tests as those used in consent to treatment issues. In the examples below, consent and access should be considered as being interchangeable.
If children are competent to give consent for themselves, consent must be sought directly from them. The legal position regarding ‘competence’ is different for children aged over 16 than those less than 16.

5.1.8.4 Children aged 16 and 17

Once children reach the age of 16, they are presumed in law to be competent to make decisions about their healthcare. This means that in many respects, they should be treated as adults and if they request access to their records at this age, and are considered competent, access should be granted.

5.1.8.5 Younger Children

[also see 5.1.8] Children under 16 are not automatically presumed to be legally competent to make decisions about their healthcare. However, some under 16s are deemed competent if they have sufficient understanding and intelligence to enable them to understand what is proposed (‘Fraser ruling/competence’). If a child of 16 or 17 is not considered competent, a person with parental responsibility can make a request on behalf of a minor. Before releasing the data, consideration must be given to the fact that the request is made solely in the interests of the minor.

5.1.8.6 Once a Child Reaches the Age of 18

If the child is deemed competent, no-one else can make decisions on their behalf. Therefore access requests cannot be made by a third party on their behalf, unless signed consent from the individual is enclosed with the request.

5.1.8.7 Children with Learning Disabilities

It must not be assumed that a child with learning disabilities is not competent to make his/her own decisions. Many children will be competent if information is presented in an appropriate way and they are supported through the decision-making process.

5.1.9 Requests from other NHS Trusts

Requests for patient information from other NHS Trusts will be required in writing to establish their lawful basis for the request and also to confirm the identity of both the requestor and the data subject. Such requests may not be accompanied by consent and in these circumstances as long as the lawful basis is noted and we are satisfied that this is legitimate, the request can be processed.

In instances where consent has not been provided and lawful basis is noted by the requestor as “in the best interests …” then it is the decision of the Trust, as data controller, whether to release the requested
information or to limit the quantity of information, and/or to redact the information as noted in paragraph 5.1.6.

As the data controller it is the decision of the Trust to disclose or withhold information requested, irrespective of the documentation or information they provide to us. It is perfectly reasonable to ask the reasons why the information is needed and what information is required before deciding whether it is appropriate for this information to be released. This is not to be obstructive but to ensure that the Trust deals with the request within the remit of the relevant legislation. The IG team will be happy to discuss any concerns you may have.

5.1.10 Police Requests/Court Orders

As with any general disclosure of information, requests from the police/court will be handled by the IG Team and advice can be obtained from the team if you should receive one.

Police Staff must not feel pressured or intimidated into giving information just because the police have requested it, in any circumstances.

The Police may submit a request made under the DPA 2018 (previously known as a S29 request). This allows the applicant to request information without consent of the individual, if the personal data is to be processed for any of the following purposes:

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders.

If the consent of the data subject cannot be obtained, the Trust requires the request to be authorised/countersigned by a chief inspector. The IG Team will ensure that all necessary information/documentation have been received from the police.

As the data controller it is the decision of the Trust to disclose or withhold information requested by the police, irrespective of the documentation or information they provide to us. It is perfectly reasonable to ask the reasons why the information is needed and what information is required before deciding whether it is appropriate for this information to be released. The IG team will be happy to discuss any concerns you may have.

Court Orders
An exception to the requirement for consent from the data subject also extends to information requested by court order.

If the Trust receive a Court Order then the IG team will work with the area to ensure that the information is provided by the date and time specified on the Order.
Only copies must be provided unless a court order is provided for originals, in which case stringent preparation of the records must take place to ensure their completeness.

Urgent requests for such information will be treated with the highest priority

5.1.11 **War Pensions and Benefits Agency**

The types of requests will be handled via the IG Team and treated like any other SAR.

5.1.12 **Indication of Litigation against the Trust**

Where there is an indication that a claim or litigation may be intended against the Trust or its employees the request will be copied to the Litigation Manager. The IG Team will continue to handle the disclosure and forward copies of documents released to third parties to the Litigation Team for their records.

5.1.13 **Safeguarding Cases**

Legislation places certain duties on local authorities where they have reasonable cause to suspect that a child or adult who lives in their area are suffering or likely to suffer significant harm. Local authorities are required to make such enquiries as they consider necessary to enable them to decide whether any action must be taken to promote an individual’s welfare.

A duty is placed upon the Trust to assist with those enquires by providing relevant information and advice about an individual if called upon to do so.

If a request for information about an individual is received in the context of proceedings to protect the vital interests of the subject, consent need not be obtained and records may be released where necessary. It is common practice for local authorities to obtain orders requiring disclosure of relevant records in the interest of a subject, for example, for the purposes of child or adult protection issues. The Court Order may require only a limited amount of documentation to be disclosed and the terms of the order must therefore be checked carefully, particularly the date which the information is to be presented to the court as this maybe a shorter timescale laid down by the DPA.

It is important that appropriate advice is sought on any access requests involving Protection issues. Staff must ensure that the IG team and safeguarding named nurses for both children and adults are contacted before any records or reports are released.
For requests made by prisons refer to the section on requests from other NHS Trusts (5.2.13).

5.1.14 **Requests made on behalf of Patients who lack Mental Capacity**

Schedule 3 Part 2(4(c) of the DPA 2018] states ‘where the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs’.

Where a request for health records is made and the data subject is a patient who lacks mental capacity, the following options are available:

- an attorney with a health and welfare lasting power of attorney (LPA) registered with the Office of the Public Guardian can make a request
  N.B. property and financial affairs LPAs and enduring powers of attorney are not acceptable for this purpose
- a personal welfare deputy appointed by the Court of Protection can make a request
  N.B. property & financial affairs deputies and appointees for benefits cannot make a request
- a one-off Court of Protection order can be made
- an Assistant Director (AD) may consent to release health records to a requestor who has indicated that a complaint or litigation claim will be made against the Trust if the AD feels it is in the best interest of the patient
- The Mental Capacity Act 2005: Code of Practice states ‘If a person lacks the capacity to consent to the disclosure, it may be acceptable and appropriate to disclose the information in the person’s best interests. Healthcare professionals should use their professional judgement to determine what is in the patient’s best interest. This should include consultation with colleagues, and the organisation's Caldicott Guardian and take into account the patient's previously expressed wishes and views’.

5.1.15 **Process for Dealing with Requests**

The IG Team are responsible for handling and recording all requests for information made under the GDPR, the AHRA, the MRA and the FOIA.

Requests can be made verbally but, as we must be satisfied as to the requestor's identity, we ask all requests to be made in writing to the Trust, and can be done so in the following ways:

(a) **letter/email**

- from data subject = must contain signature and ID;
- from 3rd party = must contain consent of data subject; or if not applicable, evidence of authority of legally designated person, ie Court of Protection Deputyship (lacks mental capacity)\l Power of Attorney (covering Health & Welfare), etc;
(b) application form - data subject
- Access to Health Records [Appendix 2i]; or
- Access to Staff Records [Appendix 2ii];
  Relevant forms of ID must accompany request as noted at Part 4
  of the application forms

(c) application form – 3rd party [Appendix 3] = must contain subject
  consent or lawful basis for making request without consent.

(d) telephone
  upon request, an application pack can be sent to requestor which
  includes relevant application form, leaflet (Appendix 4) and a prepaid
  envelope, for completion and return to the IG Team.

On receipt of a SAR the Information Governance team (IG Team) will
liaise with the relevant services. Each service area within the organisation
should have a nominated individual who has overall responsibility for co-
ordinating and ensuring all requests received are processed in
accordance with this policy. These individuals will ensure that the notes
requested are located, copied and third party information removed. [See
Appendices 9/9i].

In the event of possible none compliance with Data Protection timeframes
the IG Team will escalate the subsequent reminder to the Service Director
and the Trust’s SIRO. This reminder will be sent 1 week before the Data
Protection Act statutory deadline.

To safeguard the identity of individuals with similar, common names staff
need to carefully check requested records to ensure that they pertain to
the correct data subject throughout, eliminating the possibility of a
confused record, for example, a patient record which has been misfiled
with information relating to a patient with the same name. First line of
address, date of birth and NHS number, where applicable, must be used
to identify patients.

In addition, consent to release records form [Appendices 6i/6ii] must be
completed and signed by the lead health professional and returned to the
IG Team with the copy records. Service areas must only send copy
records to the IG Team for release to reduce the risk of incidents involving
lost original records. The IG Team will then ensure that the copy records
are released to the requestor via a secure method.

If it is agreed that the patient or their representative may directly inspect
their health records access must be supervised by a health professional
or a lay administrator. A lay administrator is a neutral person who can
oversee the viewing and ensure that the records remain safe.

In these circumstances the lay administrator must not comment or advise
on the content of the record: if the applicant raises queries an
appointment with a health professional should be offered. On completion of the inspection the records must immediately be returned to the place of storage. If the viewing is part of a SAR the IG Team must be notified.

It may be necessary to arrange for an interpreter to be present if the patient or their representative does not have English as their first language and will experience difficulties inspecting the records.

Please see process flow diagrams at Appendices 7 to 9i for more detail.

5.2 Access to Health Records Act 1990 (Deceased Persons)

5.2.1 Rights of Access

The Act provides a small cohort of people with a statutory right to apply for access to information contained within a deceased person’s health record.

There may be circumstances where individuals who do not have a statutory right of access under the Act request access to a deceased patient's record. Current legal advice is that the courts would accept that confidentiality obligations owed by health professionals continue after death. The Department of Health, General Medical Council and other clinical professional bodies have long accepted that the duty of confidentiality continues beyond death and this is reflected in the guidance they produce.

There are also a range of public bodies that have lawful authority to require the disclosure of health information. These include the courts, legally constituted public inquiries and various regulators and commissions, e.g.: the Audit Commission and the Care Quality Commission; in these cases the common law obligation to confidentiality is overridden.

The Act provides certain individuals with a right of access to the health records of a deceased individual. These individuals are the patient's personal representative and any person who may have a claim arising out of the patient’s death. A personal representative is the executor or administrator of the deceased person’s estate.

5.3 Coroner’s Office

A Standard Operating Procedure (SOP) is available via the Trust website https://www.rdash.nhs.uk/24101/standard-operating-procedure-managing-communication-from-the-coroners-office/

The purpose of this SOP is to set out a clear process within the Trust for receiving communication from the Coroner’s Office. These requests are dealt with by the Trust’s IG Team.
All correspondence from Coroner’s office should be received by the Chief Executive Office. Should any staff member receive communication from the Coroner’s Office they should immediately inform their Line Manager/Assistant Director and forward a copy to the Chief Executive’s Office.

5.4 Medical Reports Act 1988

The MRA governs access to medical reports made by a medical practitioner who is, or has been responsible for, the clinical care of the patient for insurance or employment purposes. Reports prepared by other medical practitioners, such as those contracted by the employer or insurance company, are not covered by the MRA. Reports prepared by such medical practitioners are covered by the DPA.

A person cannot ask a patient’s medical practitioner for a medical report on him/her for insurance or employment reasons without the patient’s knowledge and consent. Patients have the option of declining to give consent for a report about them to be written.

5.5 Freedom of Information Act 2000 and Access to Health Records

The Freedom of Information Act (FOIA) is a law that makes provision for the disclosure of information which is held by public authorities and those who provide services to public authorities.

The FOIA does not allow people to gain access to private sensitive information about themselves or others, such as information held in health records. Those wishing to access personal information about them should apply under the DPA.

There are specific exemptions in the FOIA to stop disclosure of personal health information:

- **Section 40** – Information that constitutes personal information under the DPA is exempt from the provisions of the FOIA if its disclosure would contravene any of the DPA principles;
- **Section 41** – Information that has been provided in confidence is exempt from the provisions of the FOIA.

5.6 Dealing with Complaints

If a subject access requestor is dissatisfied with their response or with the way in which their request has been handled, they can either request (in writing) to the Trust for an internal review; or lodge a complaint or raise any concerns about the way the Trust has handled their personal information, with the Information Commissioners Office (ICO). Either way the Information Governance Manager will investigate the ‘complaint’ and respond either to the requestor or the ICO with their findings.
Where a service user considers that their records contain inaccuracies, they must be advised to make an informal approach to the responsible health professional concerned to discuss the situation. However, it should be noted that the diagnosis is a matter of clinical judgement and cannot be changed at the service user’s request. The service user can place an addendum in his/her file with their raised concerns if the records cannot be amended.

If this avenue is unsuccessful then the service user may pursue a complaint under the Trust’s Policy and Procedure for Handling Formal Complaints in an attempt to have the information corrected or erased. They could further complain to the Information Commissioner who may rule that the information is corrected, blocked, erased or destroyed.

6. **TRAINING IMPLICATIONS**

There are no specific training needs in relation to this policy however, within the Trust Induction Programme all staff commencing employment with the Trust are made aware of this process as part of the IG training session.

The IG Team offer training to meet identified needs: this can be requested by contacting the IG Team.

As a Trust policy, all staff need to be aware of the key points that the policy covers. Staff can be made aware through the examples below.

- Team Brief
- Weekly Newsletter
- Local Induction
- Trust wide email
- Team meetings
- Special meetings

7. **MONITORING ARRANGEMENTS**

<table>
<thead>
<tr>
<th>Area for Monitoring</th>
<th>How</th>
<th>Who by</th>
<th>Reported to</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy content</td>
<td>Paper for debate</td>
<td>IG Manager</td>
<td>IG/RM Steering Group</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Timescales</td>
<td>Shared Drive</td>
<td>IG Team</td>
<td>Information Asset Owners, Deputy / Care Group Directors and Caldicott Guardian.</td>
<td>Monitoring commences at lapse of timescale for return of information to IG for each request</td>
</tr>
</tbody>
</table>

8. **EQUALITY IMPACT ASSESSMENT SCREENING**

The completed Equality Impact Assessment for this Policy has been published on the webpage of the RDaSH website – follow link https://www.rdash.nhs.uk/24095/access-to-health-records-policy-3/
8.1 Privacy, Dignity and Respect

The NHS Constitution states that all patients should feel that their privacy and dignity are respected while they are in hospital. High Quality Care for All (2008), Lord Darzi’s review of the NHS, identifies the need to organise care around the individual, ‘not just clinically but in terms of dignity and respect’.

As a consequence the Trust is required to articulate its intent to deliver care with privacy and dignity that treats all service users with respect. Therefore, all procedural documents will be considered, if relevant, to reflect the requirement to treat everyone with privacy, dignity and respect, (when appropriate this should also include how same sex accommodation is provided).

| Indicate how this will be met |
| This policy will ensure that staff handle and release patient’s information within the remit of the Laws and ensure privacy is obtained at all times. |

8.2 Mental Capacity Act

Central to any aspect of care delivered to adults and young people aged 16 years or over will be the consideration of the individuals capacity to participate in the decision making process. Consequently, no intervention should be carried out without either the individuals informed consent, or the powers included in a legal framework, or by order of the Court. Therefore, the Trust is required to make sure that all staff working with individuals who use our service are familiar with the provisions within the Mental Capacity Act. For this reason all procedural documents will be considered, if relevant to reflect the provisions of the Mental Capacity Act 2005 to ensure that the interests of an individual whose capacity is in question can continue to make as many decisions for themselves as possible.

| Indicate How This Will Be Achieved. |
| All individuals involved in the implementation of this policy should do so in accordance with the Guiding Principles of the Mental Capacity Act 2005. (Section 1) |

9. LINKS TO ANY ASSOCIATED DOCUMENTS

- Information Governance Policy
- Data Protection & Confidentiality Policy
- Corporate Records Policy/ Healthcare Record Keeping Policy
- Policy and Procedure Relating to the Handling of Formal Complaints
- Mental Capacity Act Policy

10 REFERENCES

Trust’s Policies and Procedures:
https://www.rdash.nhs.uk/category/publications/policies/corporate-policies/information/information-governance/

Department for Health’s Guide on Access to Health Records (Feb 2010)
11. APPENDICES

1 Definitions

2(i) Application form for Access to Health Records
2(ii) Application form for Access to Staff Records

3 3rd party Application form for Health Records

4 Access to Health Records Leaflet

5. Redaction Guide

6(i) Consent to Release Form relating to Health Records
6(ii) Consent to Release Form relating to Staff Records

7 Flow Chart and notes – Subject Access Requests received by IG Team

8 Flow Chart and notes – Subject Access Requests received by Service

9 Flow Chart and notes – Subject Access Request – Actions
Appendix 1

Definitions

'personal data' means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Application for Access to Health Records

Part 1 – person that the requested information relates to (the data subject)

<table>
<thead>
<tr>
<th>Title (please circle)</th>
<th>Mr.</th>
<th>Mrs.</th>
<th>Miss</th>
<th>Ms</th>
<th>Other (please specify):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Telephone No.</td>
</tr>
</tbody>
</table>

If the name and/ or address given above have changed during or since treatment, please give details:

- Previous Name(s)
- Previous Address

Part 2 – who is making this request, are you the data subject?

Yes, I am the data subject

No, I am not the data subject

Are you authorising another person to make this request on your behalf? (please circle)

- Yes
- No

If you are authorising someone to make this request on your behalf, please sign to authorise the person named in Part 3

Signature

Part 3 – details of person acting on behalf of the data subject

<table>
<thead>
<tr>
<th>Title (please circle)</th>
<th>Mr.</th>
<th>Mrs.</th>
<th>Miss</th>
<th>Ms</th>
<th>Other (please specify):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Telephone No.</td>
</tr>
</tbody>
</table>

Part 3a – nature of request being made on behalf of the data subject (the following questions do not need to be answered if the data subject has given authority in Part 2 for you to make this request)

1. Do you have legal authority to request the data subject’s information, e.g.: letter of authority, Lasting Power of Attorney? (please circle your response)
   - Yes Go to Q.2
   - No Go to Q.3

2. If you have legal authority to request the data subject’s information, have you attached proof? Your application will not be processed without proof (please circle your response)
   - Yes Go to Part 4
   - No

3. Do you have parental responsibility for the data subject who is under 16 years of age? (please circle your response)
   - Yes Go to Q.4
   - No Go to Q.5

4. If you have parental responsibility for the data subject, have you attached proof (eg child’s birth cert, court order, etc) Your application will not be processed without proof (please circle your response)
   - Yes Go to Part 4
   - No

5. Is the data subject deceased? (please circle your response)
   - Yes Go to Q.6
   - No

6. Are you the deceased data subject’s personal representative (executor or estate administrator)? (please circle your response)
   - Yes Go to Q.7
   - No Go to Q.8

Appendix 2(i)
7. If you are the deceased data subject’s personal representative, have you attached proof?  
   Your application will not be processed without proof *(please circle your response)*
   | Yes | No |
   | Go to Part 4 |

8. Do you have a claim arising from the data subject’s death? *(please circle your response)*
   | Yes | No |
   | Go to Q.9 |

9. If you have a claim arising from the data subject’s death, have you attached proof? Your application will not be processed without proof *(please circle your response)*
   | Yes | No |
   | Go to Part 4 |

### Part 4 – proof of identity *(to be completed by the data subject if making the application, otherwise to be completed by the person acting on behalf of the data subject)*

The Trust has a duty to ensure personal information is kept secure. We must be satisfied you are who you say you are. Please provide evidence of your identity by attaching copies of two of the following documents: both documents must be current and valid and show your name; at least one must also show your current address.(Please circle your attachments)

<table>
<thead>
<tr>
<th>Passport</th>
<th>Driver’s licence</th>
<th>Biometric residence permit</th>
<th>UK certificate of naturalisation</th>
<th>UK birth or adoption certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Insurance card</td>
<td>Benefits claim letter (within 3 months)</td>
<td>P45, P60 or recent payslip (within 3 months)</td>
<td>Marriage certificate</td>
<td>Divorce papers (nisi or absolute)</td>
</tr>
<tr>
<td>Student union card</td>
<td>School record</td>
<td>Letter confirming eligibility for State Pension</td>
<td>Employer ID/ letter from employer (within 3 months)</td>
<td>Medical card</td>
</tr>
<tr>
<td>VAT exemption certificate</td>
<td>Life insurance policy</td>
<td>Recent bank statement (within 3 months)</td>
<td>Recent utility bill (within 3 months)</td>
<td>Prison discharge certificate</td>
</tr>
</tbody>
</table>

If you are unable to provide two from the above we will accept a letter confirming your identity and current address from a suitable person who is a UK resident adult, has known you for at least 2 years and is not a relative. Examples of suitable persons include business owners, librarians, professionally qualified people (doctors, lawyers, teachers, etc.), police officers, bank officers, civil servants, ministers of religion, magistrates, local councillors and members of parliament/ Scottish parliament/ the National Assembly of Wales/ European parliament.

### Part 5 – litigation claims against the Trust

Is this request being made in connection with a claim against the Trust? *(please circle your response)*
   | Yes | No |

### Part 6 – details of information being requested *(to include hospital/consultant, ward/clinic, condition/illness and dates)*

### Part 7 – declaration

I certify that the information provided on this form is true. I understand that Rotherham Doncaster and South Humber NHS Foundation Trust are obliged to confirm proof of my identity. I am aware that unlawfully obtaining or attempting to obtain personal information is a criminal offence and is liable to prosecution. I confirm that *(delete as appropriate)*:

- I am the data subject
- I have the data subject’s authority / legal authority to make this claim
- I am acting with parental responsibility *(in loco parentis)* as the data subject is under 16 years of age
- I am the deceased data subject’s personal representative, executor or estate administrator
- I have a genuine claim arising from the deceased data subject’s death

Full Name

Signature

Date
# Application for Access to Staff Records

## Part 1 – person that the requested information relates to (the data subject)

<table>
<thead>
<tr>
<th>Title (please circle)</th>
<th>Mr.</th>
<th>Mrs.</th>
<th>Miss</th>
<th>Ms</th>
<th>Other (please specify):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Gender (please circle)</td>
</tr>
<tr>
<td>Current Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Telephone No.</td>
</tr>
</tbody>
</table>

If the name and/or address given above have changed during or since employment, please give details:

Previous Name(s)

Previous Address

## Part 2 – who is making this request, are you the data subject?

<table>
<thead>
<tr>
<th>Yes, I am the data subject</th>
<th>No, I am not the data subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you authorising another person to make this request on your behalf? (please circle)</td>
<td>Yes</td>
</tr>
<tr>
<td>If you are authorising someone to make this request on your behalf, please sign to authorise the person named in Part 3</td>
<td></td>
</tr>
</tbody>
</table>

## Part 3 – details of person acting on behalf of the data subject

<table>
<thead>
<tr>
<th>Title (please circle)</th>
<th>Mr.</th>
<th>Mrs.</th>
<th>Miss</th>
<th>Ms</th>
<th>Other (please specify):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Telephone No.</td>
</tr>
</tbody>
</table>

## Part 3a – nature of request being made on behalf of the data subject (the following questions do not need to be answered if the data subject has given authority in Part 2 for you to make this request)

1. Do you have legal authority to request the data subject’s information, e.g.: letter of authority, Lasting Power of Attorney? (please circle your response) | Yes | No |
2. If you have legal authority to request the data subject’s information, have you attached proof? Your application will not be processed without proof (please circle your response) | Yes | No |
3. Is the data subject deceased? (please circle your response) | Yes | No |
4. Are you the deceased data subject’s personal representative (executor or estate administrator)? (please circle your response) | Yes | No |
5. If you are the deceased data subject’s personal representative, have you attached proof? Your application will not be processed without proof (please circle your response) | Yes | No |
6. Do you have a claim arising from the data subject’s death? *(please circle your response)*  
   **Yes**  
   **No**  
   *Go to Q.9*

7. If you have a claim arising from the data subject’s death, have you attached proof?  
   Your application will not be processed without proof *(please circle your response)*  
   **Yes**  
   **No**  
   *Go to Part 4*

### Part 4 – proof of identity *(to be completed by the data subject if making the application, otherwise to be completed by the person acting on behalf of the data subject)*

The Trust has a duty to ensure personal information is kept secure. We must be satisfied you are who you say you are.  
Please provide evidence of your identity by attaching copies of **two** of the following documents: both documents must be current and valid and show your name; at least one must also show your current address. *(Please circle your attachments)*

<table>
<thead>
<tr>
<th>Passport</th>
<th>Driver’s licence</th>
<th>Biometric residence permit</th>
<th>UK certificate of naturalisation</th>
<th>UK birth or adoption certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Insurance card</td>
<td>Benefits claim letter</td>
<td>P45, P60 or recent pay slip (within 3 months)</td>
<td>Marriage certificate</td>
<td>Divorce papers ( nisi or absolute)</td>
</tr>
<tr>
<td>Student union card</td>
<td>School record</td>
<td>Letter confirming eligibility for State Pension</td>
<td>Employer ID/ letter from employer</td>
<td>Medical card</td>
</tr>
<tr>
<td>VAT exemption certificate</td>
<td>Life insurance policy</td>
<td>Recent bank statement (within 3 months)</td>
<td>Recent utility bill (within 3 months)</td>
<td>Prison discharge certificate</td>
</tr>
</tbody>
</table>

If you are unable to provide two from the above we will accept a letter confirming your identity and current address from a suitable person who is a UK resident adult, has known you for at least 2 years and is not a relative. Examples of suitable persons include business owners, librarians, professionally qualified people (doctors, lawyers, teachers, etc.), police officers, bank officers, civil servants, ministers of religion, magistrates, local councillors and members of parliament/ Scottish parliament/ the National Assembly of Wales/ European parliament

### Part 5 – litigation claims against the Trust

Is this request being made in connection with a claim against the Trust? *(please circle your response)*  
   **Yes**  
   **No**

### Part 6 – details of information being requested

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Department</th>
<th>Position held</th>
<th>Dates</th>
</tr>
</thead>
</table>

### Part 7 – declaration

I certify that the information provided on this form is true. I understand that Rotherham Doncaster and South Humber NHS Foundation Trust are obliged to confirm proof of my identity. I am aware that unlawfully obtaining or attempting to obtain personal information is a criminal offence and is liable to prosecution. I confirm that *(delete as appropriate)*:

- I am the data subject
- I have the data subject’s authority / legal authority to make this claim
- I am the deceased data subject’s personal representative, executor or estate administrator
- I have a genuine claim arising from the deceased data subject’s death

**Full Name**

**Signature**

**Date**
# 3rd Party Request for Access to Health Records

## Part 1 – Data Subject

<table>
<thead>
<tr>
<th>Title <em>(please circle)</em></th>
<th>Mr.</th>
<th>Mrs.</th>
<th>Miss</th>
<th>Ms</th>
<th>Other <em>(please specify):</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Surname</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Forename(s)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Date of Birth</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Gender <em>(please circle)</em></strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Male</td>
<td>Female</td>
</tr>
<tr>
<td><strong>Current Address</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Post Code</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Telephone No.</strong></td>
</tr>
</tbody>
</table>

If the name and/or address given above have changed during or since treatment, please give details:

| **Previous Name(s)**     |     |      |      |    |                           |
| **Previous Address**     |     |      |      |    |                           |

| **NHS Number Or Other Identifier** |     |      |      |    |                           |

## Part 2 – Details of person and/or organisation making the request

<table>
<thead>
<tr>
<th>Organisation</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title <em>(please circle)</em></strong></td>
<td>Mr.</td>
<td>Mrs.</td>
<td>Miss</td>
<td>Ms</td>
<td>Other <em>(please specify):</em></td>
</tr>
<tr>
<td><strong>Surname</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Forename(s)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Post Code</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Telephone No/ email address</strong></td>
</tr>
</tbody>
</table>

## Part 3 – Nature of request being made on behalf of the data subject

10. Please provide details of the required information

11. Please give a brief explanation of why these records are required.

12. Do you have signed consent from the patient allowing Rotherham Doncaster and South Humber NHS Foundation Trust to Share the requested information?  
   Yes  
   No  
   Please provide a copy  
   Go to Q.4

13. If you do not have explicit consent from the patient, please provide a justification for your request and the Trust will consider this under ‘best interest’ for the patient.

## Part 4 – Declaration

I certify that the information provided on this form is accurate.

| **Full Name** |     |      |      |    |                           |
| **Position** |     |      |      |    |                           |
| **Signature** |     |      |      |    | **Date**                 |
Rotherham Doncaster and South Humber NHS Foundation Trust is committed to further improving the services it provides, whilst maintaining and reaffirming your rights.

**It is your right to have access to your health records and know that everyone working for the NHS is under a legal duty to keep your records confidential.**

This leaflet informs you of what you need to do if you wish to access your health records and gives a brief explanation of what to expect.

The Data Protection Act 2018 gives all ‘living’ individuals the legal right of access to any written and/or automated health records, subject to safeguards to protect the patient and third parties.

The Access to Health Records Act 1990 gives certain people the right to apply for access to information held in a deceased person’s health records.

The Medical Reports Act 1988 gives access to medical reports made by medical practitioners for insurance or employment purposes.

It may not be necessary to make a formal application. The health care professional responsible for your care has the discretion to allow you informal access to your records.

Access is given to you, the patient or, alternatively, you may prefer to give written consent for a nominated advocate to be the one to whom access is given.

Parents of children under 16 years of age will usually have access to their child's records, however, the child's right to confidentiality must always be considered.

If a patient is not capable of managing his or her own affairs, the person appointed by the Court to manage their affairs can make an application to access the patient's health records.

There are time scales laid down by the Acts, which state that you should be given the information within a month.

In most cases we cannot charge a fee to comply with a subject access request. However, where a request is manifestly unfounded or excessive we may charge a “reasonable fee” for the administrative costs of complying with the request.

We can also charge a reasonable fee if an individual requests further copies of their data following a request. We will base the fee on the administrative costs of providing further copies.

If you wish to have access to health records you will need to complete an
application form. Please note that you will be required to provide proof of identity.

To obtain a form please contact the Information Governance Team via:
- telephone on 01302 798357;
- email at rdash.ig@nhs.net or
- in writing to Rotherham Doncaster & South Humber NHS Foundation Trust, Information Governance, Health Informatics, Woodfield House, Tickhill Road Site, Doncaster, DN4 8QN.

On receipt of the completed application form, the Information Governance Team will process the request within the time scales laid down under the appropriate legislation.

If you have any queries or require any further information, please contact a member of your care team, as they will be pleased to discuss any queries you may have. Alternatively contact the Information Governance Team direct.

Compliments and complaints

The Trust welcomes advice and suggestions about how the services might be improved.

Many problems can be easily resolved by talking with a member of your care team. If, after speaking to a member of your care team, you are still unhappy, you may wish to contact the Patient Advice and Liaison Service (PALS) by:

- telephone on 0800 015 4334 during normal office hours, Monday to Friday (excluding public bank holidays). Your telephone call will be free from a BT landline. Please note, telephone calls from other networks, for example, a mobile phone, may be charged. If you inform us that you are calling from a mobile phone, we will return your call directly; or
- email at rdash.pals@nhs.net ;or
- completing a Your Opinion Counts form. Please tell us about your experience of using our services by completing our “Your Opinion Counts” form. Alternatively, Your Opinion Counts forms are available in all public areas of Trust premises; or
- in writing to the Patient Advice and Liaison Service, Woodfield House, Tickhill Road Site, Doncaster, DN4 8QN;

If you have any further questions, please contact any member of your care team.
Redaction Guidance for Personal Data

Editing exempt information from paper and electronic documents prior to release

Redaction of health records is made only in limited circumstances whereby restricting the rights to access to ‘protect the data subject or the rights and freedoms of others’ [DPA Article 23(i)]

Redaction can only be made by an ‘appropriate health professional', one who is currently or was most recently, responsible for the care/treatment of the data subject, and where there is more than one health professional, the one who is most suitable in relation to the request.

The lawful reasons for redaction are:

1. **Third Party Information** - disclosing information about another individual who can be identified from that information [GDPR Schedule 2 (Part 3(16)], except if:
   - the other individual has consented to the disclosure; or
   - it is reasonable to comply with the request without that individual’s consent.

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:
   - the type of information that you would disclose;
   - any duty of confidentiality you owe to the other individual;
   - any steps you have taken to seek consent from the other individual;
   - whether the other individual is capable of giving consent; and
   - any express refusal of consent by the other individual.

Further factors to be considered:
   - Is the information already known to the requestor?
   - The circumstances relating to the individual making the request: the need to preserve a third party’s confidentiality must be weighed against the requestor's right to access the information;
   - Need to distinguish between a third party’s personal information and information about a third party that is also about the data subject: for example:

<table>
<thead>
<tr>
<th>Example</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. His mother suffers from depression – is personal information about a third party that cannot be released without their explicit permission</td>
<td></td>
</tr>
<tr>
<td>B. He was voluntarily accommodated as his mother is unable to cope as she is suffering from depression – is personal information about a third party and the data subject that must be redacted appropriately</td>
<td></td>
</tr>
<tr>
<td>C. He was voluntarily accommodated as his mother is unable to cope – is acceptable for release as it provides context without disclosing the third</td>
<td></td>
</tr>
</tbody>
</table>

So, although you may sometimes be able to disclose information relating to another individual, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject’s right of access against the other individual’s rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both...
information about the individual who is the subject of the request, and information about someone else [ICO Guide to GDPR (March 2018)]. Consideration should also be given to the nature of the third party and their proposed use of the information.

2. **Contrary to subject’s expectations and wishes** [GDPR Schedule 3 - Part 2(4)(2)] — disclosing information when the subject has said not to. We must respect the wishes of the data subject therefore we are unable to disclose health records if they identify information that was:
   - provided by the subject in the expectation that it would not be disclosed to the person making the request;
   - which was obtained as a result of any examination/investigation to which the data subject consented in the expectation that the information would not be disclosed; or
   - which the subject has expressly indicated should not be so disclosed

3. **Serious harm** [GDPR Schedule 3 (Part 2(2)(2)] — disclosing the information 'would be likely to cause serious harm to the physical or mental condition of the data subject, or any other person';

**Deceased Data Subjects**

Note: Data protection and confidentiality only apply to living individuals; however, it is DoH/GMC policy to treat records of the deceased with same level of confidentiality as those for the living so all applicable guidelines above must be followed.

**Staff Names**

These should be disclosed as they will only be contained within the health records within their professional capacity, although unless there is a risk to their health and safety. Their names may be released to the data subject as they are probably already known to them. Consideration should be given to any consequences or detriment of releasing staff names to third party requestors.

Names of staff from other agencies may be released if they are held by the Trust in the context of providing a complete care package. If telephone numbers are requested, switchboard numbers should be released rather than direct lines.

**Sensitive Personal Data (aka Special Category Data)**

Consent must be obtained before releasing sensitive personal information about the data subject that is not relevant to the request. Sensitive personal data consists of information pertaining to:

- Racial or ethnic origin
- Political opinions
- Sexual life
- Trade Union membership
- Physical or mental health or conditions
- Criminal Convictions
- Religious beliefs or other beliefs of a similar nature

**Third Party Opinion**

If a non-Trust professional gives an opinion it should not be released without consent from that person/ their organisation; however, we may consider releasing it without consent if it influenced the Trust’s provision of treatment and care. If the data subject is already aware of the opinion it can be released.

**Legal Privilege**

Advice provided by Trust solicitors/ legal advisors must not be disclosed. Court documents, including statements ordered by the court, are court property and cannot be released: anyone wishing to obtain them should apply directly to the appropriate court.
Self-Incrimination & Disclosure of Concerns
Information revealing evidence of an offence and exposing the Trust to criminal proceedings must not be released. If information of this nature is discovered it must be reported immediately to a manager. Where this is not appropriate or escalation is required, it should be raised with a Director or the Chair of the Trust.

Please note that this is guidance only and that each request should be dealt with on a case by case basis.

[References to DPA and GDPR related to the Data Protection Act 2018 and the General Data Protection Regulation 2016]

Further Information
Please refer to the IG Team on (01302 798357) or email rdash.ig@nhs.net

IG Intranet site (staff only):  http://nww.intranet.rdash.nhs.uk/support-services/health-informatics/information-governance/accessing-personal-information-subject-access-request/

IG Public Website - https://www.rdash.nhs.uk/support-and-advice/information-governance/how-do-i-access-personal-information/
Consent to Release Health Records under the
Data Protection Act 2018/General Data Protection Regulations 2016
/Access to Health Records Act 1990

This consent form must be signed by:

- The health professional who is currently, or was most recently, responsible for the clinical care of the data subject in connection with the information that is the subject of the request; or
- Where there is more than one such health professional, the health professional who is the most suitable to advise on the information that is the subject of the request.

Note: if the health professional has left the organisation the current or most suitable health professional must advise on the information that is the subject of the request.

I (name) ....................................................................................... of (dept.) ........................................................................

confirm that I have viewed the health records of the data subject whose details are as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current/ Last Known Address</th>
<th>NHS Number</th>
<th>Date of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Names or Aliases (if applicable)</td>
<td>Previous Addresses (if applicable)</td>
<td>Date of Death (if applicable)</td>
<td></td>
</tr>
</tbody>
</table>

And (tick box):

- I authorise the release of the requested information to the applicant (if consent covers more than one RDASH service's records/notes, please identify the other RDASH services)

- I authorise limited release of the requested information to the applicant because (give details)

- I do not authorise the release of the requested information to the applicant because (give details)

(Please note that a reason for not releasing requested information is required for Information Governance purposes and will not be disclosed to the applicant)

Declaration

By signing this form I am agreeing that:

- A copy of the information, for which I have authorised the release, is attached and the original information has been returned to the place of storage
- The attached copy information pertains to the correct data subject, the details of whom are shown above
- Third party information, for which we do not have consent to release, has been removed from the attached copy information
- Information that is likely to cause serious harm to the physical or mental health of the data subject or another person has been removed from the attached copy information

Signed: ................................................................. Date: ..........................
Consent to Release
Staff Records under the
Data Protection Act 2018 and
General Data Protection Regulations 2016

This consent form must be signed by:
• The person who is currently, or was most recently, responsible for the data subject in connection with the information that is the subject of the request; or
• Where there is more than one such person, the person who is the most suitable to advise on the information that is the subject of the request.

Note: if the person has left the organisation the current or most suitable person must advise on the information that is the subject of the request.

I (name)…………………………………………..………………... of (dept.) ……………………………………… confirm that I have viewed the records of the data subject whose details are as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Service/Dept</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

And (tick box):

☐ I authorise the release of the requested information to the applicant (if consent covers more than one RDASH service’s records/notes, please identify the other RDASH services)

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

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

☐ I authorise limited release of the requested information to the applicant because (give details)

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

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

☐ I do not authorise the release of the requested information to the applicant because (give details)

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

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

(Please note that a reason for not releasing requested information is required for Information Governance purposes and will not be disclosed to the applicant)

Declaration

By signing this form I am agreeing that:
• A copy of the information, for which I have authorised the release, is attached and the original information has been returned to the place of storage
• The attached copy information pertains to the correct data subject, the details of whom are shown above
• Third party information, for which we do not have consent to release, has been removed from the attached copy information
• Information that is likely to cause serious harm to the physical or mental health of the data subject or another person has been removed from the attached copy information

Signed: ……………………………………………………. Date: ……………………………………
Request Received: Although can be either verbal or in writing, but to confirm the identity of the requestor (if received verbally), you will need to obtain identification documentation, therefore an application pack should be sent out. The statutory timeframe under the DPA 2018 for completion of a request (from receipt of ‘complete’ request) is ONE month, definition of which has yet to be confirmed, therefore the Trust deems to this to be 28 calendar days.

Log: All requests and subsequent contacts/correspondence are logged on the Trust’s Safeguard database by the IG Team, including scanned copy of request and service submissions.

Complete Appl: In order to process requests, the following is required:
- Details of the data subject, ie name, date of birth;
- Proof of ID (if data subject)
- Requestor’s signature/declaration
- Details of the requestor (if not the data subject)
- Consent of data subject – if able to do so
- Supporting info (if requestor is not the data subject), ie legal authority
- Details of the requested information

Complete – NO: write to requestor, confirming receipt and outstanding requirements. Clock on database is stopped until outstanding documentation is submitted and in order. Once this information is received and in order, the Clock is started and the request process begins.
Complete – YES: Process request.

When advising a requestor that we will NOT be complying with a request, there is no legal requirement to give the reason why, however, best practice is to offer an explanation which must be recorded for IG purposes.

Fees: Copies of information must be provided free of charge, however a ‘reasonable’ fee can be levied if the Trust finds the request ‘manifestly unfounded’ or ‘unreasonable’, particularly if it is repetitive. These fees are for administrative costs only, ie paper, postage, therefore discuss with requestor if you can provide information in a different manner than hard copy, ie electronically, eg encrypted pen drive/CD, etc. Also discuss with requestor to see if the quantity could be reduced, ie rather than asking for ‘all’ records, it may be that only records from a certain service or clinician, may be relevant.

A repeat request is one that is made after the Trust has previously complied with an identical or similar request from the same person – for the same information, and when deciding if a reasonable interval has elapsed, consideration must be given to the following:
- The nature of the requested information;
- The purpose for which the information is held; and
- The frequency at which the data is added to

Acknowledge: Letter sent to requestor, confirming receipt and that request is being processed, also gives statutory timeframe under the Act and IG Team contact details. At this point it may be known if fees are applicable, so the requestor should be made aware, so that they can decide whether to pursue or withdraw their request.

Action: Each request will be actioned by the designated person, usually service manager or team leader, who will act as handler for SARs, the request will also be sent to their admin support (or admin generic email)
Request received by Service

Verbally (phone)
- transfer to IG/take details and forward to IG
- log request/consent, actions and release on patient’s record
- ensure secure release
- deal with direct

In person
- take details and forward them to IG
- redirect requestor to IG
- Deal with direct

In writing/email
- forward to IG
- deal with direct

Appendix 8
Request Received: Requests can be either verbal or in writing, but to confirm the identity of the requestor, you will need to obtain identification documentation. It is advisable to obtain any request in writing (dated and signed), so that we have an audit trail and something to forward to the respective service/staff member to process. [See Appendices 2i/2ii] for a copy of the current Request to Health/Staff Records Application Form

Method of Receipt: Although you will need to consider the method of receipt in deciding which of the above you choose, ie:
- **Verbally** - In these instances you need to ensure that the person on the end of the phone is who they say they are, which can be difficult and unless you are 100% sure, you are advised to follow one of the other options. You must never give any personal information over the phone if cannot confirm the identity of the caller, as this will breach data protection/confidentiality;
- **In person**, this could be at the reception desk or it could be during a treatment session with clinician/keyworker. If the latter applies, ID/authority should not be an issue as you will already know them, again if dealing with direct, you would need to ascertain their identity, and if not the data subject, their legal authority to apply on the data subject’s behalf.
- **In writing/email** – email to rdash.ig@nhs.net / in writing to The Information Governance Team, Woodfield House, Tickhill Road Site, Balby, DN4 8QN

Method of Process: Irrespective of the method of receipt, there are four main ways to deal with the request:
- **Deal with direct** - ensure ID has been confirmed/authority has been established and that request, actions and release are logged on data subject’s patient record. All records should be released securely if not released in person, ie postal [recorded/special delivery] or email [encrypted/password protected];
- **Transfer to the IG Team** (01302 798357 or rdash.ig@nhs.net);
- **Take details and pass on to the IG Team**, ie requestor’s name and contact telephone number, and tell them that you will forward to the IG Team for them to make contact and discuss request process. It is also helpful if you can obtain the date of birth of the data subject to aid identifying the correct person; or
- **Give requestor IG Team contact number** (above)

NOTES:
The statutory timeframe under the DPA 2018 for completion of a request (from receipt of ‘complete’ request) is ONE month, definition of which has yet to be confirmed, therefore the Trust deems to this to be 28 calendar days.

Refusing a request - there is no legal requirement to give the reason why, however, best practice is to offer an explanation which must be recorded for IG purposes. You are advised to contact the IG Team to discuss possible grounds for refusal, or if dealing with direct, rather than refuse you may wish to contact the requestor to discuss possibility of restricted or limited release/response if applicable.

Fees - copies of information must be provided free of charge, however a ‘reasonable’ fee can be levied if the Trust finds the request ‘manifestly unfounded’ or ‘unreasonable’, particularly if it is repetitive. These fees are for administrative costs only, ie paper, postage, therefore discuss with requestor if you can provide information in a different manner than hard copy, ie electronically, eg encrypted pen drive/CD, etc. Also discuss with requestor to see if the quantity could be reduced, ie rather than asking for ‘all’ records, it may be that only records from a certain service or clinician, may be relevant.

A repeat request is one that is made after the Trust has previously complied with an identical or similar request from the same person – for the same information, and when deciding if a reasonable interval has elapsed, consideration must be given to (i) the nature of the requested information; (ii) the purpose for which the information is held; and (iii) the frequency at which the data is added to.
ACTION SENT TO APPLICABLE SERVICES (by IG Team)

services check databases for requested information

ARCHIVES
- retrieve
- print a copy
- return originals to archives

CURRENT
- retrieve/print
- check and redact (if applicable)
- Submit to IG Team

Target Date Set [14 calendar days] for service to submit to the IG Team

Target Date [calendar days]:
- 1-14 days = 
- 14-21 days = 
- 21-28 days = 
- 28+ days =

IG Team send reminder emails to outstanding services

IG Team escalate to Care Group Director

notify IG Team if request found to be 'manifestly unfounded' or 'excessive'

IG Team to contact requestor to discuss request

Appendix 9
**Timeframes:** Statutory timescale provided by Article 12(3) of the General Data Protection Regulations 2016 (GDPR) states within one ‘month’ of receipt of the request. Currently there is definition of a month, therefore as advised by the ICO this Trust has adopted for a 28 day period to ensure compliance is always within a calendar month.

**Extensions:** Article 12(3) also make reference to extending the statutory timeframe but only when taking into account the complexity and number of the requests.

**Fees:** Article 12(5) also deems a fee may be charged where requests are found to be ‘manifestly unfounded’ or ‘excessive’ (again no definitions given, so judgement is made by Trust). Excessive could be repetitive in nature, etc. The fee should be reasonable and take into account the administrative costs of providing the information or communication or taking the action requested. At this point, once IG have been made aware that this may be applicable to a request, the IG Team have two options: (i) charge a fee; or (ii) refuse. Whichever option the IG Team will make the requestor aware and if they refuse to pay the fee, then the request will be refused.

**Target Dates**
- 1-14 days (calendar) = half way target date - will be notified to respective services [identified on safeguard database as GREEN];
- 14-21 days (calendar) = weekly reminder email sent to outstanding services [identified on safeguard database as YELLOW];
- 21-28 days (calendar) = more frequent reminder emails sent to outstanding services [identified on safeguard database as ORANGE];
- 28+ days (calendar) = outside statutory timeframe – daily reminder emails sent – copy in Care Group Director (CGD) [identified on safeguard database as RED];

At the Orange timeframe – if services have notified IG that they may not meet deadline, a letter/email is sent to requestor releasing records ready to release with apology for not completing within timeframe. If request is NOT complex, then CGD is made aware.

**Records Retrieval:** services are required to check BOTH paper and electronic records AND in certain circumstances, archived records. Access to archive databases must be requested from the Trust’s Records Manager. The action email will usually list the services/dates for information, but services are required to double check for themselves. Service to ensure the records relate to the respective patient (checking NHS/DOB, etc) once confirmed, to print a copy and return original file to wherever they obtain it from.

**Redaction:** There are two reasons redaction may be applicable and in both instances the decision must be undertaken by a health professional, who is either currently or was most recently, responsible for the data subject: (i) the ‘serious harm test’ in relation to ascertaining whether releasing information if it would be likely to cause serious harm to the physical or mental health of the data subject or another” [Schedule 2-Part 3 of the Data Protection Act 2018]; and (ii) removal of third party information ie “disclosing information relating to another individual who can be identified from the information.” [Schedule 2 – Part 3 of the Data Protection Act 2018] - Note - Trust redaction guidance and training is being drafted and will be rolled out in due course.

Services MUST only submit records that relate to the request, no more-no less, unless they have reason to withhold. In these instances the consent to release form must be completed, ticking the correct option (2 and 3 for limited or refusal to release) AND explanation why must be entered.