Data Protection, Caldicott and Confidentiality Policy

Subject Access Requests and Disclosure of Personal Data Procedure

Version: 10

Summary: Procedure to ensure compliance with the Data Protection Act to manage access to personal information by data subjects and disclosure of personal data.

Keywords (minimum of 5): (To assist policy search engine) Data Subject Requests, Access to Records Leads, Subject Access

Target Audience: All staff who contribute or manage clinical information – both paper and electronic.

Next Review Date: May 2020 – annual review

Approved and ratified by: Information Governance Group

Date of meeting: 13 May 2019

Date issued: May 2019

Author: Liz Bega, Records Manager

Sponsor: Karl Marlowe, Medical Director and Caldicott Guardian
### Version Control

**Version 7 2017 Amendments Summary:**

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2.6</td>
<td>Amended the generic email address provided from the Information Assurance Inbox, to the Access to Records inbox</td>
</tr>
<tr>
<td>6</td>
<td>4.2</td>
<td>Added in information relating to the central log held on the subject access sharepoint and the need for the Access to Records Leads to complete this, as well as the detailed logs held locally.</td>
</tr>
<tr>
<td>10</td>
<td>4.10</td>
<td>Sentence amended as per request from Finance to state ‘when the appropriate fee, made payable to Southern Health has been received’</td>
</tr>
<tr>
<td>16</td>
<td>15</td>
<td>Address of the Caldicott Guardian and Head of Legal Services amended.</td>
</tr>
</tbody>
</table>

**Version 8 2018 Amendments Summary:**

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1.1</td>
<td>Changes regarding GDPR</td>
</tr>
<tr>
<td>5</td>
<td>2.3-2.4</td>
<td>Slight amendment to wording around complaints/incidents</td>
</tr>
<tr>
<td>6</td>
<td>3.3-3.4</td>
<td>Addition of sections regarding the GDPR and the main changes to the access to records process</td>
</tr>
<tr>
<td>7</td>
<td>4.2</td>
<td>NHS Code of Practice 2006 amended to 2016</td>
</tr>
<tr>
<td>9</td>
<td>4.7</td>
<td>Addition of statement advising staff who work/worked in integrated teams with Adult Services to contact the Records Team if they are unsure of the correct information sharing SOPs/MOUs</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>GDPR added to list of references</td>
</tr>
</tbody>
</table>

### Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Page</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/09/2015</td>
<td>R Lloyd</td>
<td>V6</td>
<td>6</td>
<td>Section 21: Update with correct Divisional title</td>
</tr>
<tr>
<td>25/11/2015</td>
<td>R Lloyd</td>
<td>V6</td>
<td>1</td>
<td>Change procedure title</td>
</tr>
<tr>
<td>16/12/2015</td>
<td>R Lloyd</td>
<td>V6</td>
<td>10</td>
<td>Viewing manual records – correction to charging scale.</td>
</tr>
<tr>
<td>16/12/2015</td>
<td>R Lloyd</td>
<td>V6</td>
<td>16</td>
<td>Disclosure Exemptions under the Data Protection Act 1998</td>
</tr>
<tr>
<td>16/12/2015</td>
<td>R Lloyd</td>
<td>V6</td>
<td>All</td>
<td>Update references to SARs Toolkit documents and letters</td>
</tr>
<tr>
<td>25/10/2016</td>
<td>R Lloyd</td>
<td>V6</td>
<td>7</td>
<td>Amend charging &amp; fee scale</td>
</tr>
<tr>
<td>12/04/2017</td>
<td>L Bega</td>
<td>V7</td>
<td>5</td>
<td>Email address change</td>
</tr>
<tr>
<td>12/04/2017</td>
<td>L Bega</td>
<td>V7</td>
<td>6</td>
<td>Information added regarding central sharepoint log</td>
</tr>
<tr>
<td>12/04/2017</td>
<td>L Bega</td>
<td>V7</td>
<td>10</td>
<td>Finance information added</td>
</tr>
<tr>
<td>12/04/2017</td>
<td>L Bega</td>
<td>V7</td>
<td>16</td>
<td>Address changes</td>
</tr>
<tr>
<td>02/03/2018</td>
<td>L Bega</td>
<td>V8</td>
<td>As above</td>
<td>See above for detail – key changes relate to changes in the law with the introduction of the GDPR</td>
</tr>
<tr>
<td>June 2018</td>
<td>L Bega</td>
<td>V9</td>
<td>All</td>
<td>Addition of DPA 2018, and rewording to reflect changes in timescales (one month) and definitions. Updated front cover</td>
</tr>
<tr>
<td>02/11/2018</td>
<td>L Bega</td>
<td>V9</td>
<td>6, 10</td>
<td>Further information added surrounding process to be followed when consideration is being given to withholding information where a request is ‘manifestly unfounded or excessive’ Removed V6 amendment summary</td>
</tr>
<tr>
<td>20/12/18</td>
<td>Liz Bega</td>
<td>V9</td>
<td>7, 13</td>
<td>Minor amendments regarding the process for clinical disclosure and clinical sign off.</td>
</tr>
<tr>
<td>29/04/2019</td>
<td>Donna Woolley</td>
<td>V9</td>
<td>6</td>
<td>Legacy name change: generic email from HP-TR. to SHFT</td>
</tr>
<tr>
<td>01/05/2019</td>
<td>Lesley Barrington</td>
<td>V10</td>
<td>7 (4.1) / 17 (16)</td>
<td>Update to wording Update to references</td>
</tr>
</tbody>
</table>

### Reviewers/contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Version Reviewed &amp; Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emma Peckham</td>
<td>Subject Access Administrator</td>
<td>V5 d0.1 / August 2011</td>
</tr>
<tr>
<td>Lesley Barrington</td>
<td>Head of Information Assurance</td>
<td>V7 DV0.01 27/7/2015</td>
</tr>
<tr>
<td>Mark Williams</td>
<td>Business Support Manager</td>
<td>V7 DV0.01 19/08/2015</td>
</tr>
<tr>
<td>Sarah Pearson</td>
<td>Head of Legal &amp; Insurance Services</td>
<td>V7 DV0.01 27/08/2015</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td></td>
<td>V7 16/09/2015</td>
</tr>
<tr>
<td>Information Commissioner’s Office Audit Team</td>
<td></td>
<td>V7 20/10/2015</td>
</tr>
<tr>
<td>Liz Bega</td>
<td>Records Manager</td>
<td>V7 12/04/2017 V8 02/03/2018</td>
</tr>
</tbody>
</table>
# CONTENTS

<table>
<thead>
<tr>
<th>Section:</th>
<th>Subject:</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Introduction and key timescales</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>Access to Records Leads (ATRL)</td>
<td>5</td>
</tr>
<tr>
<td>3.</td>
<td>Timescale for Complying with Requests</td>
<td>6</td>
</tr>
<tr>
<td>4.</td>
<td>Processing a Subject Access Request</td>
<td>7</td>
</tr>
<tr>
<td>6.</td>
<td>Disclosure – Other than directly to the Data Subject</td>
<td>12</td>
</tr>
<tr>
<td>7.</td>
<td>Disclosure Exemptions</td>
<td>14</td>
</tr>
<tr>
<td>8.</td>
<td>Medical Act 1983</td>
<td>14</td>
</tr>
<tr>
<td>9.</td>
<td>Court Orders, Coroners Courts &amp; Criminal Cases Review Commission</td>
<td>15</td>
</tr>
<tr>
<td>10.</td>
<td>War Pensions and Benefit Agency</td>
<td>15</td>
</tr>
<tr>
<td>11.</td>
<td>Mental Health Review Tribunals</td>
<td>15</td>
</tr>
<tr>
<td>12.</td>
<td>Medical Reports Act 1998</td>
<td>15</td>
</tr>
<tr>
<td>13.</td>
<td>Patient Living Abroad</td>
<td>16</td>
</tr>
<tr>
<td>14.</td>
<td>Filing of Subject Access Requests</td>
<td>16</td>
</tr>
<tr>
<td>15.</td>
<td>Useful Contacts</td>
<td>16</td>
</tr>
<tr>
<td>16.</td>
<td>References Further Information</td>
<td>17</td>
</tr>
<tr>
<td>17.</td>
<td>Supporting Documentation</td>
<td>17</td>
</tr>
</tbody>
</table>
Subject Access Requests and Disclosure of Personal Data Procedure

1. Introduction

1.1 This procedure has been written to assist all staff with a responsibility for dealing with requests for personal data from a Data Subject (the individual whom particular personal data is about). These will be known as Subject Access Request (SAR).

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and the Data Protection Act 2018 now applies.

Information must be disclosed within one month following the date of receipt, and organisations will no longer be able to charge data subjects for requesting their information.

The Trust must act on the subject access request without undue delay and at the latest within one month of receipt. The Trust should calculate the time limit from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Examples provided by the Information Commissioner’s Office in interpreting these guidelines are as follows:

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond. This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply. For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

In certain circumstances personal data may be disclosed, for example, when an exemption is applied under the General Data Protection Regulation/Data Protection Act 2018, there is a legal duty or a Data Sharing Agreement or Protocol is in place. This type of request is not a Subject Access Request but it is recommended that each request is individually assessed of the need to disclose the information and document that the information has been released to whom for what reason. The Subject Access Request framework can be used to record and process these types of request.

1.2 Except in the case of a deceased individual, the Access to the Health Records Act 1990 has been repealed and access to all records for living individuals now comes under the General Data Protection Regulation/Data Protection Act 2018.

1.3 Individuals (Data Subjects) have a right:

- be informed whether personal data is processed (which includes being held or stored);
- a description of the data held, the purposes for which it is processed and to whom the data may be disclosed;
- a copy of the information constituting the data;
- information as to the source of the data.
1.4 This Procedure does not cover in any detail requests for records generated by Coroner’s Inquests or Police Enquiries. Please refer to the Head of Legal Services for advice upon receiving such requests.

1.5 Where integrated Hampshire County Council (HCC)/Southampton City Council (SCC)/other City Councils and Southern Health NHS Foundation Trust (SHFT) teams are in operation in mental health or learning disability services, the Trust manages the access process – and reviews the content of the record. If the record contains information that is outside the remit of the provision of mental health care (e.g. Safeguarding Adults/Children Case Conference Minutes/information; other assessments carried out by Adult Services), permission to disclose must be sought from the author/organisation/agency, as with all other 3rd party information. Each agency is responsible for giving permission for the disclosure of its information.

1.6 This procedure relates to legislation as set out in the General Data Protection Regulation/Data Protection Act 2018., covering the use of personal data. The Freedom of Information Act 2000 relates to non-personal information and legislation will give individuals the right to access non-personal information held by the NHS from January 2005.

If an application for personal data is made under Freedom of Information for either alive or in respect of the deceased, the application should be managed under the Data Protection Act or Access to Health Records Act and the requestor informed.

2. Access to Records Lead (ATRL):

2.1 Medical/Clinical Records

All Trust staff should forward requests for copies of health records to the nominated Access to Records Lead.

In the Mental Health, Older Persons Mental Health and Learning Disabilities, each site and/or service will nominate an ‘Access to Records Lead’ to handle access requests. The Access to Records Lead (ATRL) will follow the procedure as set out in this document and associated Toolkit.

For Integrated Community Services and Childrens Services the Subject Access Administrator, based at Lymington Hospital will manage the process.

2.2 Human Resources (HR)

If a member or ex-member of staff requires a copy of his/her personal data, the request should be made directly to the HR Access to Records Lead.

2.3 Customer Experience Team

If an individual requires access to his/her personal data regarding complaints/concerns, the request should be made to the Customer Experience Team.

2.4 Ulysses Safeguard (Incident reports)

If an individual requires access to his/her personal data – specifically incident reports or investigation reports - the request should be made to the Serious Incident Requiring Investigation, Incident and Risk Team.

2.5 Access to CCTV records

Please refer to SH NCP 57 Closed Circuit Television (CCTV) Policy for further information.
2.6 All other requests/enquires

All other requests or enquiries to be directed to the Records Team – shft.accesstorecords@nhs.net

3. Timescale for complying with Subject Access Requests

3.1 The Data Controller (i.e. the Trust) should comply with the request promptly, preferably within 21 days but no later than one month after the request has been made. Whilst there is no actual penalty for not complying with the one month time period, the person making the request has the right to complain to the Information Commissioner, who may respond with an “improvement notice” or fine to the Trust.

3.2 Under the Access to Health Records Act 1990, if the record has been updated during the 40 days preceding the access request, access must be given within 21 days of the request. Where the record concerns information all of which was recorded more than 40 days before the application, access must be given within one month with no fee. As with the General Data Protection Regulation/Data Protection Act 2018, organisations should endeavour to supply the information within 21 days.

3.3 Organisations will no longer be able to charge a fee for processing a request for records. However, organisations can charge a ‘reasonable fee’ in circumstances where a request is deemed manifestly unfounded or excessive, particularly if it is repetitive (Section 53 of the Data Protection Act 2018). A reasonable fee may also be charged to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

The period for compliance can be extended by a further two months where requests are complex or numerous. If this is the case, the individual MUST be informed within one month of the receipt of the request and explain why the extension is necessary. Please see 1.1 for further details regarding timescales.

In the rare event that the service is considering withholding information under Section 53 of the Data Protection Act 2018 (Manifestly unfounded or excessive requests by the data subject) the Records Manager and Head of Information Assurance should be consulted in the first instance.

The request may then be escalated to the Executive Lead for the service to confirm that this exemption has been applied appropriately, and that there is evidence to support this decision. The Data Protection Act 2018 states that the data-controller (the Trust) is responsible for demonstrating that the request is manifestly unfounded or excessive. The data-controller must therefore record the reasons for a decision to restrict (whether wholly or partly) the rights of the data-subject, and make the record available to the Information Commissioner, if requested to do so.

If the Exemption is applied, then the service will seek support from the Records Manager in informing the data-subject;

(a) that their rights have been restricted,
(b) of the reasons for the restriction,
(c) of their right to make a request to the Commissioner under section 51,
(d) of their right to lodge a complaint with the Commissioner, and
(e) of their right to apply to a court under Section 167.

(Section 45 (5) of the Data Protection Act 2018)
4. **Processing a Subject Access Request**

4.1 **What is a subject access request?**

A subject access request is a request made by or on behalf of an individual for the information which he or she is entitled to ask for under Article 15 of the General Data Protection Regulation 2018. The request does not have to be in any particular form. Nor does it have to include the words ‘subject access’ as long as it is clear that the individual is asking for their own data. The Requester does not have to make any reference to the General Data Protection Regulation/Data Protection Act 2018, the request may be a valid subject access request even if it refers to other legislation, such as the Freedom of Information Act.

The General Data Protection Regulation 2018 does not specify how to make a valid request. Therefore, an individual can make a subject access request verbally or in writing. It can also be made to any part of the Trust (including by social media) and does not have to be made to a specific person or contact point.

What should you do if someone makes a request for their information?

- If you know the requester, pass their request to the relevant Access to Records Lead.
- If you do not recognise the requester, ask the requester for proof of identity (e.g. valid passport, driving licence, birth certificate or named utility bill) and inform them that the Trust will formally respond to their request once their identity has been verified.
- Once you have endorsed the requester’s identity - pass the request to the relevant Access to Records Lead immediately.

4.2 **Log Sheet / File**

An individual log/tracking sheet will be started by the ATRL to track the request in detail through the service, detailing the date the request was received and when each stage of the request was completed.

Copies of relevant correspondence and/or documentation in connection with the request will be placed in a file and maintained by the ATRL.

The ATRL will also ensure that any request for records is logged and tracked via the Trust Central Subject Access Request log on the Sharepoint site. If the ATRL does not have access to this, they should contact the Records Team.

A check must be made of previous requests to ensure that a ‘reasonable’ time (at least 6 months) has elapsed since any previous request from the same individual. If further clarification is required – contact the Records Manager or Head of Legal Services.

The NHS Code of Practice – Records Management 2016 – states that “Subject access requests (GDPR and AHR – records of requests) must be kept for 3 years after last action and destroyed under confidential conditions” or for 6 years if the request was appealed.

4.3 **Letter in Reply**

A letter or email of acknowledgement will be sent to the requester. The letter may also include the Trust’s subject access application form should any aspect of the request require clarification.

4.4 **Request for further information**

**Identity:** to comply with the law, information relating to the Data Subject must only be disclosed to that person (data subject) or someone with their written consent to receive it.
Please refer to section 6, Disclosure – Other than directly to the Data Subject for further information on disclosing to third parties and children.

Adequate steps must be taken to identify the requestor before commencing the work to comply with the request under the act.

Where there is any doubt, proof of identity will be required. Examples of suitable documentation could include copies of:

- Valid Passport.
- Driving Licence.
- Birth Certificate along with some other proof of address, e.g. a named utility bill or a Medical Card.

If the originals of these documents are received, the Trust must take due care of them and ensure their safe return (i.e. using Recorded Delivery or similar). A photograph of the applicant is not necessary. Please refer to SH IG 42 Policy for the Management of Personal Information (Section 5.1) with regards risk assessing how to send the documents.

**Details:** to enable a search of the records, sufficient details are required, for example, data subject’s name, previous name, date of birth or NHS number. The ‘Subject Access Application Form’ may be sent to the Data Subject enabling clarification of the information required.

### 4.5 Reply Received

When a reply is received from the Data Subject in response to any request for further information, this will be checked by the ATRL to ensure that it is satisfactory and adequate to continue the process.

### 4.6 Search for data/files

The ATRL will circulate a ‘Subject Access Search Memo’ – refer to the Subject Access Request Toolkit, to all registered holders of data (i.e. the relevant Corporate department or service’s Team or Ward Manager) to search for both manual and electronic information.

The registered holder will be responsible for checking systems (including computer held records), emails and files for any reference, directly or indirectly, relating to the Data Subject. Please remember that the GDPR/DPA 2018 does not permit you to exclude information from your response simply because the information is difficult to access.

The Data Subject is entitled to a “legible, understandable and intelligible” copy of the records – and the onus is on the Data Controller (i.e. the Trust) to comply. At its most basic, this means the information should be understandable by the average person (*Subject access code of practice – Information Commissioner’s Office*). Therefore if any entry needs to be re-typed – the responsibility for this lies with the relevant Department, service or Team. A glossary of terms should be provided to the requester wherever possible.

Copies of the information will be obtained via printing, photocopying and returned to the ATRL dealing with the request. In some instances, data is held in an electronic system which you are unable to print off as a document. So you may need to take screen shots of the information to convert to a PDF document in order to provide a printed copy.

Once the search is complete, the registered holder or holders of data must complete the ‘Subject Access Search Memo’ to inform the ATRL of the outcome – even if no records are found.
4.7 Withholding Information (review of data/files)

Some or all information may be withheld if it is:

- Third party
- Could cause serious harm to the physical or mental health or condition of the Data Subject, or any other person (refer to the Exemption from Article 15 of the GDPR – Serious Harm)
- Legal Privilege – information that relates to legal advice is classed as legally privileged and is therefore exempt from the GDPR provisions

4.8 Definition of a Third Party:

There are generally two components to the meaning of third party:

- A person who has provided information (about the data subject)
- An organisation, other than the data controller (the Trust) or data processor (the Trust or authorised organisation that processes data on behalf of the Trust) that has provided information (about the data subject)

Information provided by a third party, for example, neighbour, friend, family member, employer, Police, teacher, play group assistant, other agencies – DVLA, Benefits Agency, about the service user is classed as ‘Third Party Information’.

This could also be data from a third party organisation, for example Police, Social Services, School and DVLA

With regards to third party information, please consider the following points:

- Does the request require the disclosure of information that identifies a 3rd party? Consider whether it is possible to comply with the request without revealing information that relates to and identifies a 3rd party individual.
- Has the 3rd party individual consented? Good practice to contact 3rd parties and request consent.
- Would it be reasonable in all the circumstances to disclose without consent? Has the data subject already had a copy of the information? Consider if a genuine duty of confidence is owed to the 3rd party, for example, the information is not available to the public and has been shared with the expectation it will remain confidential.

The ICO Subject Access Code of Practice three-step approach to dealing with information about third parties provides further guidance to assist with deciding whether to disclose information relating to a third party. Please apply a case by case approach when reviewing third party information.

**Medical Records only - Important**: Where information is found as to the physical or mental health or condition of the Data Subject, then disclosure cannot be made without reference to an appropriate health professional (Exempt from Article 15 of the GDPR (Serious Harm))

The designated person (ATRL) will seek the consent of the appropriate Health Professional/Consultant/Department Manager for the release of the records. For clinical records, this will be the person currently or most recently responsible for the clinical care of the Data Subject to which the information relates, or where more than one is involved, the two or three clinicians most knowledgeable on that disclosure. In circumstances where the clinician has left the organisation and existing clinicians have not had contact with the Data Subject, this should be escalated by the ATRL to the most senior clinician or the clinician who feels most able to review the records. The Data Protection Act 2018
outlines that this review must be undertaken by a Health Professional, and therefore this cannot be delegated to administrative staff.

For non-clinical records this will be the Director or Associate Director. In less complex cases or where it is felt appropriate, non-clinical information requests can be delegated to team manager level, or whomever is deemed sufficiently senior to review the information. When the information sought is complex or particularly sensitive, the advice of the Information Assurance Team and/or Caldicott Guardian should be sought.

Where services are or were integrated with Adult Services – particular care must be taken to ensure that the partner agency has been informed of the access request – and that an appropriate clinician/manager from the partner agency has reviewed the file. This is particularly relevant when reviewing information held on HCC/SCC Information Systems [SWIFT/PARIS]. Please consult the Records Team to seek access to the Memorandum of Understanding in the event of a request for records.

Should the registered holder decide that disclosure would be harmful to the Data Subject or any other person, the reasons for this must be clearly documented, as a Court Order seeking disclosure might subsequently be sought by the Data Subject or his/her representative. This should be recorded on the “Confirmation of Disclosure Memo” – refer to the Subject Access Request Toolkit, and forwarded to the ATRL – who will record this on the log sheet. The reason why this has not been disclosed must also be communicated to the data subject, although a full clinical risk assessment must also be undertaken and recorded within the Access Request process, and in the clinical records.

The data-controller must record the reasons for a decision to restrict (whether wholly or partly) the rights of the data-subject, and make the record available to the Information Commissioner, if requested to do so.

The service will inform the data-subject;

(a) that their rights have been restricted,
(b) of the reasons for the restriction,
(c) of their right to make a request to the Commissioner under section 51,
(d) of their right to lodge a complaint with the Commissioner, and
(e) of their right to apply to a court under Section 167.

(Section 45 (5) of the Data Protection Act 2018)

4.9 Legal Privilege

Legal Professional Privilege protects all communication between a professional legal adviser and his or her clients from being disclosed without the permission of the client.

The privilege is that of the client and not that of the professional legal advisor. This type of data is exempt from the right of subject access requests.

Please contact the Head of Legal Services for further information.

Please refer to SARs Toolkit for Consent to 3rd Party Letter and Disclosure Memorandum.

4.10 Collating Responses/Redaction

The ATRL will collate the information received and prepare the disclosure response to the Data Subject as necessary.

The purpose of redaction is to irreversibly remove the exempt information from the final copy. Please remember to redact information using a safe and secure process, for
example, black marker, Banner Correction Roller (correction tape), tipex or Microsoft Office functionality.

NB: Remember to keep a record of what information has been removed and why, for example, legal privilege.

Please refer to the SARs Toolkit, ICO Guidance, ICO – How to disclose information safely – redaction advice

4.11 Sending Copies of Data – disclosure of information

When the information is complete and agreed/signed off – a copy of the record can be made. Copies of the information and a covering letter will then be sent by Recorded Delivery to the requestor by the ATRL.

If information has been withheld due to third party considerations, legal privilege or potential harm to the individual or others – this must be communicated to the requestor in the covering letter. Please refer to SARs Toolkit for the Disclosure Letter

The requestor may ask for the information to be disclosed to them over e-mail. This can be done, but a disclaimer must be sent to and signed by the data subject.

The statement below can be included in any of the standard letters in the appendices as required.

You have also requested that we send a copy of your record electronically to (email address); we are happy to share information in this format but we would like to remind you that the information would not be encrypted and cannot guarantee that this is a secure method of delivery nor accept responsibility if the email does not reach you. We therefore ask that if you wish us to send your record this way that you sign the disclaimer below and send to us prior to us sending the record.

“I would like to request a copy of my health records sent to my email account and understand Southern Health NHS Foundation Trust cannot guarantee that this is a secure method of delivery nor accept responsibility if the email does not reach me.

Name: ___________________  Signature: ___________________
Date: ___________________  Email address: ___________________

4.12 Supervised access to view records

Viewing the records/information is an option but only if both parties agree. If not, copies will be provided as above.

If viewing is supported – the process of reviewing the data sources and records must take place as before (with the removal of third party information). The information/records must not be left unattended with the requestor – so the registered holder of data must remain in the room at all times to ensure the records are not tampered with and to explain any entries or terminology; or to decipher and help with any legibility queries.


The AHRA 1990 only relates to information relating to deceased persons.
For access to records relating to the deceased, applications may only be received from:

- the service user’s personal representative, and
- any person who may have a claim arising from the service user’s death.

The status of next-of-kin does not give the requestor any automatic rights with regards to being granted access to the deceased records.

However access is NOT to be given to the record or any part of it, if:

- a note is included in the record that the service user did not wish access to be given, or
- the service user had given the information and would not have expected it to be disclosed, or
- it would disclose information that is not relevant to any claim.

Information will be required to establish a link between the requester and the deceased. A copy of the death certificate (executor of will), a copy of the letter of administration and a description as to the relationship with the person making the request or valid reason for access should be sought.

On occasion, research organisations will request access to the records as part of the research project. Access can only be approved to relevant information with the prior written consent of the deceased person, or their personal representative.

6. Disclosure - Other than directly to the Data Subject

6.1 Information may be requested by third parties (e.g. solicitors, relative, Ofsted etc.) on behalf of the Data Subject. Where this is accompanied by authorisation (documented consent) from the Data Subject then this request can be processed using this procedure.

6.2 Where the request clearly states that no litigation is intended against the Trust or its employees, disclosure may take place without reference to the Head of Legal Services. If the letter indicates a claim or likely claim, a copy of the request should be sent to the Head of Legal Services who will also require a copy of the disclosed documentation. This will enable them to be fully prepared to take appropriate action in the investigation and defence of the claim.

6.3 Where the disclosure request is made by a third party on behalf of a Data Subject who lacks capacity, further advice should be sought from the Health Care professional. The registered holder must be satisfied that disclosure would be in the Data Subject’s best interests. If this is not the case, disclosure cannot proceed.

6.4 The Mental Capacity Act 2005 provides a statutory framework to empower and protect people who are not able to make their own decisions. A key principle of the law is that every adult has the right to make their own decisions and is assumed to have capacity to do so unless it is proved otherwise. Further guidance is available in the Trust's Mental Capacity Act 2005 Policy.

6.5 Under the Mental Capacity Act 2005 – Independent Mental Capacity Advocates (IMCAs) have rights of access to health/clinical records relating to the service user they are representing. The Trust (responsible body) must “give access to relevant records when requested by an IMCA under Section 35(6)(b) of the Act”. This includes “the right to examine, and take copies of any records that the person holding the record think are relevant to the investigation/decision (for example, clinical records, care plans, social care assessment documents or care home records)”. Ref: Mental Capacity Act 2005 – Code of Practice. Therefore disclosure may occur without the service user’s explicit consent.
6.6 The revised Mental Health Act (1983) 2007 (as amended) introduced the Independent Mental Health Advocate (IMHA). They are entitled to access information relating to some individuals who are subject to the Mental Health Act, and will apply by contacting the Ward Manager.

6.7 Where necessary, the third party may be contacted for additional details to enable an effective search for the information required for their purpose.

6.8 A person with parental responsibility has the right to request a copy of a child’s health record if the child is deemed competent to give consent for themselves; consent should be sought directly from them. The legal position regarding ‘competence’ is different for children aged over and under 16.

6.9 **Children aged 16 and 17:** The Mental Capacity Act covers and empowers children aged 16 and 17 (‘young persons’). A young person has capacity unless it is established he or she lacks it. If a young person lacks capacity because of an impairment of, or a disturbance in the functioning of, the mind or brain, the Mental Capacity Act will apply in the same way as it does to adults (people aged 18 or over). However if the young person is unable to make a decision for another reason, for example, because he or she is overwhelmed by its implications the common law principles set out in Gillick will apply.

6.10 **Younger Children:** 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 him or her to understand what is proposed (‘Fraser ruling/competence’ or ‘Gillick 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.

A recent report from NHS England – safeguarding Vulnerable people in the NHS – accountability and Assurance framework State:-

When children, or those with parental responsibility for them, reject measures that could save them from significant harm, their wishes can be overridden. This is part of the statutory principle that makes the welfare of the child the paramount consideration subject to that, decision-making power relating to children lies with those who have parental responsibility for the child.

However, when a child understands fully the choice to be made and its consequences, based on the Gillick competency, the child's decision prevails.

6.11 **In England, Wales and Northern Ireland, once a child reaches the age of 18** they are assumed to be a competent adult and capable of making informed decision. Therefore access requests cannot be accepted by a third party on their behalf without their consent.

6.12 **Children with learning disabilities:** it should 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.

6.13 Occasionally, requests for information will be received from other NHS or Healthcare providers, where the Data Subject has been referred into their services. This is known as a “Clinician to Clinician disclosure”. Healthcare providers generally operate on the basis of implied consent to share patient data for the purposes of direct care, without breaching confidentiality. However, each request must be considered on a case by case basis. The organisation requesting the information must be explicit about the specific information they require, and why. If they are requesting the information without the consent of the Data

SH IG 12 Subject Access Requests and Disclosure of Personal Data Procedure
Version: 10
May 2019
Subject, they will need to specify under which legal basis they are requesting the information (such as vital interests, public task or legitimate interests).

For information regarding sharing information, please refer to **SH IG 48 Information Sharing Staff Guidance**.

### 7. Disclosure Exemptions under the General Data Protection Regulation/Data Protection Act 2018

The General Data Protection Regulation/Data Protection Act 2018 recognises there may be valid reasons for not disclosing personal data; these are referred to as exemptions. In these circumstances, the disclosure of information may not be viewed as subject access request providing the exemption was valid. Therefore, this type of request must be considered on a case-by-case basis ensuring only the relevant information is disclosed to satisfy the exemption requirements.

#### 7.1 Crime and taxation:

The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following reasons:

- the prevention and detection of crime or
- the apprehension or prosecution of offenders
- the assessment or collection of tax or duty

Any request from the Police must be in writing to comply with the General Data Protection Regulation/Data Protection Act 2018. The Hampshire Constabulary DP2 form, or similar, should be produced prior to access being granted. All sections must be completed by the Police prior to submission. If a DP2 is not produced, consent from the data subject should be obtained prior to processing the request. Please remember to confirm the identity of the person representing themselves as a Police Officer, for example, ask to see their warrant card.

If the police are asking for access to the victim’s records, consideration must be given to informing the victim of the request to release information so they understand the possible consequences of a future court case where this information may be shared.

Original health records must not be given to the Police without the authorisation of the relevant Director of Operations and/or Records Manager. A copy must always be retained by the Trust and arrangements made to track the return of the originals.

#### 7.2 Other Requests

The same exemption can be applied to other organisations that have crime prevention or a law enforcement function. For example, Department of Work and Pensions – Benefit Fraud Section, NHS Fraud Department (NHS Act 2006)

In both these instances, the Trust will not charge for copies of health records.

Refer to **SH IG 47 Disclosure of Information to the Police Procedure** for further information.

### 8. Medical Act 1983

The Medical Act 1983 sets out the basic legislative framework for the governance of the
General Medical Council (GMC). The Medical Act gives the GMC powers and responsibilities, under Section 35A for taking action when questions arise about fitness to practice. As part of fitness to practice investigation, the GMC may request access to medical records. The registered holder must comply with this request and have 14 days (Section 35 A (6A)) to process and provide copies of the information held. In these instances, the Trust will not charge for copies of health records.

9. Disclosure required by statute - Court Orders, Coroners Courts & Criminal Cases Review Commission

9.1 All Court Orders and associated documents must be immediately forwarded to the nominated ATRL for processing. Authorisation will be requested from the registered holder involved and photocopies of the records given to the Court. If required, advice will be taken from the Head of Legal Services. The originals will not be sent without the authorisation of the relevant Clinical Lead or Division Lead.

9.2 Coroners do occasionally ask for records. The registered holder needs to negotiate with the Coroner whether they want the originals, and if so, a copy of the record should be made prior to disclosure. The Coroner is entitled to the originals and they are the only people that the Trust will release the originals to. However, if the Coroner will accept a copy, then that can be supplied.

9.3 Access to clinical records requested by the Criminal Cases Review Commission is via Criminal Appeal Act 1995, section 17(2). This is a statutory duty, and consent from the service user is not required. All information held by the Data Controller must be disclosed as requested. For further information guidance contact the Records Manager.

In the event of the originals being handed over, a complete copy of the records, documents, files must be made and retained by the registered holder.

10 War Pensions and Benefit Agency

10.1 All requests received will be directed to the registered holder for their authorisation or completion. Originals will not be sent; copies must be taken and forwarded. In accordance with HSC 1999/001, copies of records will be supplied without charge and requests should aim to be met within ten working days of receipt.

11. Requests connected to Mental Health Review Tribunals

It is acknowledged that a number of requests for access are received in preparation for Mental Health Review Tribunals. The tribunals have to be arranged within a set time frame. Relevant staff are aware that such requests have to be dealt with urgently and they make every effort to ensure copies are provided in a timely fashion.


The Access to Medical Reports Act 1998 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 Act. Reports prepared by such medical practitioners are covered by the Data Protection Act 2018.
The patient can apply for access to the report at any time before it is supplied to the employer/insurer, subject to certain exemptions. The medical practitioner should not supply the report until this access has been given, unless 21 days have passed since the patient has communicated with the doctor about making arrangements to see the report. Access incorporates enabling the patient to addend to the report and providing the patient with a copy of the report.

Once the patient has had access to the report, it should not be supplied to the employer/insurer until the patient has given their consent. Before giving consent, the patient can ask for any part of the report that they think is incorrect to be amended. If an amendment is requested, the medical practitioner should either amend the report accordingly, or, at the patient’s request, attach to the report a note of the patient’s views on the part of the report which the doctor is declining to amend. Patients should request amendments in writing. If no agreement can be reached, patients also have the right to refuse supply of the report.

Medical practitioners must retain a copy of the report for at least 6 months following its supply to the employer/insurer. During this period patients continue to have a right of access.

The medical practitioner is not obliged to give access to any part of a medical report whose disclosure would in the opinion of the practitioner:

- cause serious harm to the physical or mental health of the individual or others,
- indicate the intentions of the medical practitioner towards the individual,
- identify a third person, who has not consented to the release of that information or who is not a health professional involved in the individual’s care.

A medical practitioner may make a reasonable charge for supplying the patient with a copy of the report.

13. **A patient living abroad**

When a patient moves abroad, their records will be retained by the Trust for the recommended period specified in Records Management Code of Practice for Health and Social Care 2016.

Patients who move outside the UK are not permitted to take their health records with them, however, they are entitled to request a copy of their records, and then take a copy abroad with them.

14. **Filing of Subject Access Requests**

The log and all documentation relating to a particular request should be kept and retained for a period of three years.

A copy of the disclosure letter which sets out the outcome of the request, must be retained on the data subjects record (third party section), for example, medical record, personnel file, as a record of what was disclosed/withheld. This must be retained in accordance with the required retention period.
15. **Useful contacts:**

- Caldicott Guardian: Sterne 7-8, Tatchbury Mount.
- Head of Legal Services: 6 Sterne Road, Tatchbury Mount.
- Records Manager: 1 Sterne Road, Tatchbury Mount
- Head of Information Assurance: Tidbury Farm, Sutton Scotney

16. **References / further reading:**

- General Data Protection Regulation 2018
- Data Protection Act 2018
- Access to health records Act 1990
- Medical Reports Act 1998
- The Medical Act 1983
- Requesting amendments to health and social care records – guidance for service users, service users and professionals – National Information Governance Board for Health and Social Care – December 2009
- Information Commissioners Office – [https://ico.org.uk](https://ico.org.uk)
- NHS Digital: [https://digital.nhs.uk/](https://digital.nhs.uk/)
- HSC 1999/001: The provision of patient information by NHS Trusts to the Department of Social Security requests for information used for benefit assessment purposes
- BMA Access to health records April 2019
- GMC confidentiality good practice May 2018

17. **Supporting documentation:**

The Subject Access Request Toolkit contains all the referenced forms, memos and sample letters within this procedure. The Toolkit also provides additional supporting information and other sample documentation provided by the Trust's ATRL's.