## Document Control Sheet

<table>
<thead>
<tr>
<th>Document Title / Ref:</th>
<th>Access to Records Standard Operating Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Executive Director</td>
<td>Director of Strategy, Transformation and Performance</td>
</tr>
<tr>
<td>Author and Contact Number</td>
<td>Head of Information Governance and Records 0161 882 1081</td>
</tr>
<tr>
<td>Type of Document</td>
<td>Procedure</td>
</tr>
<tr>
<td>Broad Category</td>
<td>Corporate</td>
</tr>
<tr>
<td>Document Purpose</td>
<td>To ensure the Trust has in place policy and procedure for handling access to records in line with Data Protection Act</td>
</tr>
<tr>
<td>Scope</td>
<td>All Staff who handle subject access requests or who may receive requests for access to personal information for both service users and/or staff</td>
</tr>
<tr>
<td>Version number</td>
<td>V4</td>
</tr>
<tr>
<td>Consultation</td>
<td>None required</td>
</tr>
<tr>
<td>Approving Committee</td>
<td>I&amp;IT Committee</td>
</tr>
<tr>
<td>Approval Date</td>
<td>January 2014</td>
</tr>
<tr>
<td>Ratification and Date</td>
<td>Lead Executive Approval – Director of Strategy, Transformation and Performance</td>
</tr>
<tr>
<td>Date of Ratification</td>
<td>16 January 2014</td>
</tr>
<tr>
<td>V1 Valid from Date</td>
<td>February 2009</td>
</tr>
<tr>
<td>Date of Last Review</td>
<td>January 2014</td>
</tr>
<tr>
<td>Date of Next Review</td>
<td>January 2016</td>
</tr>
<tr>
<td>Procedural Documents to be read in conjunction with this document:</td>
<td>Access to Records Policy</td>
</tr>
<tr>
<td>Training Needs Analysis Impact</td>
<td>All staff are required to familiarise themselves with this policy</td>
</tr>
<tr>
<td>Financial Resource Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### Document Change History

**Changes to this document in different versions must be detailed below. Rationale for the change should also be given**

<table>
<thead>
<tr>
<th>Version Number / Name of procedural document this supersedes</th>
<th>Type of Change i.e. Review / Legislation / Claim / Complaint</th>
<th>Date</th>
<th>Details of Change and approving group or Executive Lead (if done outside of the formal revision process)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Records Policy V3 Review</td>
<td>January 2014</td>
<td>Amended format to be in new Trust format for policy documentation</td>
<td></td>
</tr>
</tbody>
</table>

### External references used in the creation of this document:

If these include monitoring duties upon the Trust for this policy the specific details should be recorded on the Monitoring and Compliance Requirements sheet.

- Information Governance Toolkit v11, HSCIC 2013

### Privacy Impact Assessment submitted

| 16/06/11 - no major changes       | Any issues? | None |

---

Page 2 of 22
Policy authors are asked to consider each of the nine protected characteristics under the Equality Act 2010. We expect you to demonstrate that throughout the policy process you have had regard to the aims of the Equality Duty:

1. Eliminate unlawful discrimination, harassment and victimisation and any other conduct prohibited by the Act;
2. Advance equality of opportunity between people who share a protected characteristic and people who do not share it; and
3. Foster good relations between people who share a protected characteristic and people who do not share it.

Please provide a brief account of how you have done this, further work to be completed and any support you have had in considering the aims and working in compliance with the Equality Duty.

If you are unclear on how to do this or would like further advice and support then you may contact quality.admin@mhsc.nhs.uk.

It is the responsibility of the approving group to ensure this statement reflects the Trusts objectives and position with compliance as set out within the NHS Equality Delivery System.

This version of this policy was subject to a full equality and diversity impact assessment in line with the Equality Duty which was approved by the Equality and Diversity Committee. The Equality Duty has however been considered during the review of the policy but as the policy changes are very minor they do not have any impact the policy complies with the Equality Duty.

In line with the Trust values we may publish this document on our External Website. Is there any reason you would prefer this is not done?

No

It is the Authors responsibility to ensure all procedural documents comply with the Trust values.

If you are unclear on any of the requirements in the document control sheet then please email quality.admin@mhsc.nhs.uk before proceeding.
### Monitoring and Compliance Requirements Sheet

For audit, Registration and NHSLA purposes all procedural documents must have monitoring requirements or key performance indicators set by the authors, Committees or Lead Directors. This allows the Trust to routinely monitor the effectiveness and impact of their procedural documents on a regular basis.

<table>
<thead>
<tr>
<th>Procedural Document Title:</th>
<th>Access to Records Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does this procedural document offer support or evidence for the Trusts registered activities and outcomes?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is this an NHSLA Document?</td>
<td>No</td>
</tr>
<tr>
<td>Specify where the requirement originates</td>
<td>IG Toolkit Version 11 - HSCIC</td>
</tr>
<tr>
<td>Minimum Requirement / Standard / Indicator to be monitored &amp; Section of document it appears</td>
<td>Process for monitoring</td>
</tr>
<tr>
<td>Level 2 - 11-105 \ 1b – Policies Policy, approvals, procedure and guidelines in place</td>
<td>Review</td>
</tr>
<tr>
<td>CQC Records Outcome 21 - This outcome is about ensuring that patient records are accurate, fit for purpose, held securely and remain confidential</td>
<td>Audit</td>
</tr>
</tbody>
</table>

NB: If you have selected audit you should complete the required audit registration form and standards document and submit these with your expected timescales for completing the audit to quality.admin@mhsc.nhs.uk as soon as possible and no later than 4 weeks prior to the audit commencing.

The Group / Committee should also ensure the monitoring work is added to their yearly schedule of monitoring and action logs as appropriate.
Access to Records Standard Operating Procedure

1. Introduction

The Data Protection Act 1998 became effective from 1st March 2000, and superseded the Data Protection Act 1984 and the Access to Health Records Act 1990 and governs all subject access requests. The exception to this is the records of deceased persons, which are still governed by the Access to Health Records Act 1990.

The Data Protection Act 1998 (Section 7 – Subject Access), gives every living person or their authorised representative, the right to apply for access to their personal records irrespective of when they were compiled.

The Data Protection Act 1998, also gives patients who now reside outside the UK, the right to apply for access to their former UK health records.

As a general rule a person with parental responsibility also has the right to apply for access to their child’s health record.

The Information Commissioners Office is the statutory body, which has been established to perform various functions under the Data Protection Act 1998. They have a website with useful guidance around the Act [www.ico.gov.uk](http://www.ico.gov.uk). Alternatively, to view the Act, visit the HMSO website [www.opsi.gov.uk](http://www.opsi.gov.uk).

2. Scope

In the context of this procedure, a record is anything, which contains information (in any media format), which has been gathered as a result of any aspect of work of NHS employees or contractors in relation to patients, clients, service users or staff.

A record can be recorded in a computerised or in a manual form or a mixture of both. They may include, hand-written notes, letters, medical reports, complaints, applications, references, videos and tape-recordings of telephone conversations.

3. Definition

Within the Data Protection Act 1998 a health record is defined as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.

A health record can also be recorded in a computerised or in a manual form or a mixture of both. They may include, hand-written clinical notes, letters to and from other health professionals, laboratory reports, radiographs and other imaging records e.g. X-rays and not just X-ray reports, printouts from monitoring equipment, photographs, ECG recordings, videos and tape-recordings of telephone conversations.

The Data Protection Act 1998 is not confined to health records held for the purposes of the National Health Service. It applies equally to the private health sector and to health professionals’ private practice records. It also applies to the records, for example, of employers who hold information relating to the physical or mental health of their employees if the record has been made by or on behalf of a health professional in connection with the care of the employee.
The definition of “processing” under the 1998 Act in relation to information or data, means obtaining, recording, holding the information or data or carrying out any operation or set of operations on the information or data including:

a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available,
d) alignment, combination, blocking, erasure, or destruction of the information or data.
e) lawful processing under the 1998 Act also requires compliance with the common law duty of confidentiality where patient data is concerned.

The data subject is the individual who is the subject of personal data – e.g. the patient/service user/employee

4. Informal Access To Records

4.1 Health Records
The Trust encourages informal or voluntary arrangements whereby patients/clients, during or at the end of their treatment are able to ask to see what has been recorded about them during their episode of care within the Trust. For this reason patients/clients or their carers may (with the clients consent), with the approval of the clinician (e.g. Psychiatrist, nurse, health adviser, psychologist or other health care professional) be allowed to view their records in relation to this period of treatment.

Informal access is subject to non-disclosure of information, that may result in serious harm to the patient or other individual or may identify third parties from entries in the records.

Should the patient/client wish to be provided with copies of their records then they should be advised that they will need to apply for Formal Access to their records.

4.2 Personnel Records
Records held within the Human Resources Department are normally available to the member of staff concerned, providing always that reasonable notice has been given to the Trust. Generally, personnel records will be held and maintained by individual line managers to whom initially requests should be directed.

When a member of staff of the Trust wishes to be provided with copies of their records, they need to apply for Formal Access.

(Note: Records may also held by Occupational Health Departments and the Payroll Department on behalf of the Trust.)
5. **Formal Access To Records**

5.1 **Health Records**

Formal Access to Health records is granted by way of an Access Request form (appendix A) being completed by the patient or their representative (where appropriate) and submitted to the Trust along with the corresponding fee. Once permission has been granted by the clinician(s) and the fee has been received in full then the records may be released to the patient/client or their appointed representative.

The clinician(s) may decide that either full access or limited access may be granted to the records and this should be indicated to the Medico/Legal Clerk on the appropriate form.

If limited access is granted to the records then a letter stating this must also be sent to the patient/client and the reasons for granting only limited access should be clearly stated.

In any event the request for Access to Records should aim to be dealt with in full within 21 days of the request and the appropriate fee having been received.

Where necessary the Subject Access Officer has the discretion to waive the fee required by the Trust for Access to records. This however should only be done in cases where it would be prohibitively expensive for the patient/client to pay such fees after having taken into account the patients/clients ability to pay.

Where a patient/client has been granted access to their records under the DPA 1998 and considers that some of the information is the records is inaccurate (i.e. incorrect, misleading or incomplete) then they may apply to the custodian of the records to have necessary corrections made. If the custodian of the records is satisfied that the information is inaccurate then they must arrange to have the necessary correction(s) made. If, however, the custodian is not satisfied that the record is incorrect then they must place a note at the appropriate point in the notes of the part of the record which is considered by the patient/client to be incorrect. In either of these two cases the custodian must then provide to the patient/client a copy of the correction or note placed in the records.

5.2 **Personnel Records**

Formal Access to records, (being supplied with a copy of the records), held by the Human Resources Department is granted by way of an Access Request form being completed and returned to the Trust Human Resources Department along with the corresponding fee. Once the fee has been received in full then the records may be released to the staff member or appointed representative.

6. **Types Of Records Covered**

One of the main differences between the Data Protection Act 1984 and the Data Protection Act 1998 (DPA) is that the 1998 Act now covers both computerised and manually held records. As a consequence, the DPA has repealed the Data Protection Act 1984 and it has also repealed the Access to Personal Files Act 1987 and most of the Access to Health Records Act 1990.

Access to records of deceased patients is still covered by the Access to Health Records Act 1990.
7. **Data Controller Obligations**

The Trust is a data controller because it holds and processes data about the individuals for whom it provides services for. Therefore, the Trust has a number of obligations under the DPA on receiving a written request for access to personal records (this includes any request received by electronic means e.g. e-mail or facsimile).

The Trust must inform the individual requesting access if they, or someone else on their behalf, is processing that individual’s personal data.

If so, the individual should be given a description of:

- The personal data being held and processed such as medical records, social care records, letters, memos etc.
- The purpose for which the data are being held and processed – such as providing health care for the individual, research, audit etc.
- Those to whom the data may be disclosed to, such as health care professionals, social workers, police and courts (only in certain circumstances), general practitioners etc.

Individuals requesting access to their information are also entitled to be told of the fee that may be charged by the Trust for providing them with a copy of their records.

Subject access requests must be dealt with promptly and in any event within 40 days (The Secretary of State for Health subsequently declared that the NHS should substitute this to within 21 days as per Access to Health Records Act) of receipt of the information needed to identify the person making the request and the appropriate fee.

The person requesting information should also be told in an intelligible manner of all the information that forms any such personal data.

Whenever possible the information should be provided in a permanent form by way of a hard copy and if any of the information in the copy is not intelligible without explanation, the person requesting the information should be given an explanation of that information.

In exceptional circumstances, if it is not possible to comply within the forty-day period the applicant should be informed.

The Subject Access Officer will keep a log and will make checks to ensure that the above time frames are adhered to.

8 **Data Protection Principles**

The Data Protection Act 1998 establishes a set of principles with which the Trust as a user of personal information must comply. These are;

1. Personal information must be processed fairly and lawfully
2. Personal information should only be processed for the purpose for which it was originally given.
3. Personal information should be adequate, relevant and not excessive for the purpose for which it is processed
4. Personal information should be accurate and kept up to date.
5. Personal information should not be kept any longer than is necessary for the purpose for which it was collected,
6. Personal information should be processed in accordance with the rights of those about whom information is collected (the data subject).
7. Appropriate security measures should be in place to protect personal information.
8. Personal information should not be transferred outside the EC without ensuring the country to which the data is being transferred has adequate safeguards or without the consent of the data subject.

9. **Charging**

The DPA 1998 Subject Access Regulations gives the right to levy a fee of up to £50 for providing a copy of the medical record held in paper format and £10 for medical records held in electronic format. In relation to Social Care Records there is also a maximum fee of £10 for providing a hard copy of the record.

If a data subject wishes to view their record, either Mental Health or Social Care then the Trust may levy a flat fee of £10 for granting such access. If however, information has been added to the service users record(s) within the last 40 days then no fee may be charged. After having viewed the record(s) the data subject may ask for a hard copy of their record(s) and in such cases the fees listed below are applicable.

When subject access requests are made the Trust should take into account the applicant's ability to pay and other circumstances, and if appropriate should waive the fee. This is at the discretion of the Subject Access Officer

9.1 **Fees Explained**

Under the terms of the DPA 1998 and subsequent Statutory Instruments laid down by Parliament the fees for Access to Records charged by Manchester Mental Health & Social Care NHS Trust are as follows;

i) For providing hard copies of Computerised Records £10.00 (statutory maximum).

ii) For Providing hard copies of all or part of manually held paper records the fees shall be calculated on a sliding scale (detailed below);
   a. Up to 10 A4 pages = £15.00
   b. Between 11 and 30 A4 pages = £21.00
   c. Between 31 and 50 A4 pages = £30.00
   d. Over 50 A4 pages = £50.00 (statutory maximum)

iii) For a combination of computerised and manually held records the statutory maximum allowed is £50.00 and accordingly the fees for these records will be calculated on the sliding scale listed in (ii) above.

iv) For “Supervised Access”, simply to allow the data subject or their representative to view the manual or computerised records there shall be a standard fee of £10.00 as allowed by legislation. This fee does not allow the applicant to be given copies of the records to take away.

The above fees listed in paragraphs i – iii are inclusive of postage and all administrative fees. However charges could be waived or reduced if the health professional feels this is appropriate.

Under usual circumstances a patient currently being seen by the service will not be expected to pay a fee for viewing their records but could be asked to pay 25p per photocopy for any copies requested.
10. **Patients Living Abroad Requiring Access to their Health Records**

Former patients living outside of the UK, who once had treatment during their stay here still have the same rights, under the DPA 1998, to apply for access to their UK health records. Such a request should be dealt with as someone making an access request from within the UK.

11. **Subject Access requests made by or on behalf of children**

All individuals have the right to make subject access requests. Section 66 of the Act provides that a person under 16 may exercise any right under the Act when he has a general understanding of what it means to exercise that right and that a person of 12 years or more shall be presumed to be of sufficient age and maturity to have such understanding. A child may, of course, reach sufficient maturity earlier and it will be a question of fact in each case.

Accordingly, a data controller who receives a subject access request on behalf of a child will need to judge whether the child understands the nature of the request. If the child understands, he or she is entitled to exercise the right, using Form A(1), and the data controller should reply to the child.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child, using Form E and to receive the response.

Parental Responsibility is defined in The Children Act 1989 as ‘all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his/her property. Each parent who has parental responsibility is entitled to make decisions about the child independently of the other, although they should always consult each other about important decisions. One parent may have acquired the right to look after the child by a Residence Order. This parent will take all the day-to-day decisions about the care of the child but should always consult the other parent about important decisions. Any difficulties can be referred to the Court. A person with parental responsibility will have the right to apply for access to a child’s health record, although disclosure may be refused where the child is “Gillick Competent” and refuses to give consent.

11.1 **Third Party Information**

A data controller cannot refuse access on the grounds that the identity of a third party would be disclosed in cases where the information is contained in a health record and the third party is a health professional who has compiled or contributed to the health record or who has been involved in the care of the patient in his capacity as a health professional. If it is considered by the Trust that should such third party information be made available to the data subject that this would lead the data subject or the/a third party to suffer harm then the information may be withheld.

If the record contains information obtained from a third party or about a third party or a third party may be recognisable from the data within it, then that information should not be disclosed to the person making the request unless

a) The third party, who is not a health professional, gives their consent to the disclosure of that information.

b) It is reasonable to dispense with that third party’s consent (taking into account duty of confidentiality owed to that individual, any steps to seek his or her consent, whether he or she is capable of giving consent and whether...
consent has been expressly refused). This would be the exception rather than the rule and should be very carefully considered.

Health professionals, under the Data Protection Act 1998, are not required to approach a third party for disclosure, but in some cases they may wish to do so.

Some examples of where a third party may be involved:

a) A parent may apply for access to their fourteen-year-old child’s health records. The child may have made some reference to his / her parents (the third party), which has been recorded within their health record, but which the child did not want disclosing. The doctor may withhold this information from the child’s parents.

b) A son (the third party) visits the doctor as he is concerned about his elderly mother, who is having problems with memory loss and self care. The doctor makes notes in the mother’s health records of the visit, but if for any reason the mother decided to apply to access her health records, the doctor may withhold any information within her health records leading to the identity of her son’s visit, unless the son gave his consent to do so.

Where the Trust is satisfied that the data subject will not be able to identify the other person from the information to be disclosed, taking into account any other information which the Trust reasonably believes is likely to be in or to come in to the possession of the data subject, then they must provide the information.

13. Requests other than from The Service User

Some individuals may appoint an agent to make a request on their behalf. The Trust must obtain evidence of the agent’s authority and confirm their identity and relationship to the individual. Evidence is required in writing. Agents may be a solicitor or a person acting under a general power of attorney.

If someone lacks the capacity to manage their affairs, a person acting under a court protection order or under an enduring power of attorney can request access on that person’s behalf.

If the request is made for access to records of a deceased service user then this still falls within the Access to Health Records Act 1990, but the request may only be made by a personal representative of the deceased or by someone who may have a claim arising out of his/her death.

13.1 Elected Representatives

Under the paper “The Data Protection (Processing of Sensitive Personal Data)(Elected Representatives) Order 2002” Elected Representatives, i.e. MP’s, MEP’s, Elected Members of Local Authorities and Elected Mayors etc. may legitimately request information relating to a patient of the Trust, who is also one of their constituents, without the explicit consent of the data subject to release such information by the Trust. Such requests should be dealt with in accordance with the remainder of this policy but only if it is understood from the request from the Elected Representative that s/he is acting on the instructions of the data subject.

As a general principle it is good practice for the trust to provide such elected representatives with copies of the Trust form “Request for Access to Records” in order that this may, if possible, be completed and returned to the Trust for ALL access requests.
13.2 **Courts**

A Court may order disclosure of a patient’s health record (e.g. under the Civil Procedure Rules, the Data Protection Act 1998, etc). A Court Order should be obeyed unless there is a robust justification to challenge it, in which case, the Trust may challenge the order through the Court. The Court’s decision is law, unless the Trust decides to appeal the order and take the case to a higher court in an attempt to override the court’s decision.

A court order should not be confused with a request from a solicitor.

Courts and Coroners are entitled to request original records. If they do, copies of the records must be retained by the Trust. Coroners normally give sufficient notice for copies to be made, but have the power to seize records at short notice, which may leave little or no time to take copies.

**ONLY on explicit direction of the Judge to the representative of the Trust should Casenotes be handed over to the Court or to a third party as directed by the Judge. Casenotes should be handed over with a copy of the Trust's letter for Judges (see appendices).**

There are many scenarios surrounding Courts and access to Health Care Records and advice should always be sought if a member of staff receives a request for Casenotes where there is any doubt as to how to deal with the request. If the matter is complicated then the Trust will have the opportunity to speak with the Trust’s solicitors.

**If an affidavit or court order is issued to the Trust it must immediately be telephoned through to the Corporate Services Manager or the Information Governance Manager at Trust Headquarters. Following this, the affidavit or order must be faxed to the manager above.**

13.3 **Solicitors**

Solicitors frequently act on behalf of patients and staff in doing so require and regularly request access to personal information for example Casenotes and medical reports etc. Providing that the Solicitors request is both in writing and is accompanied by a letter of authority signed by the patient or staff member authorising the solicitor to have access to his/her records, this must be current and not older than 6 months, this should satisfy the requirements of the Data Protection Act. However Casenotes and medical reports may only be released after the consultant or health care professional has agreed to such release, either unrestricted or restricted; and on receipt of the appropriate fee from the client/solicitor.

Under no circumstances should original records be sent to solicitors. The Trust should only ever send photocopies.

13.4 **Police**

The Trust wants to foster good working relations with the police as well as wishing to be seen playing its part in protecting the public from crime.

At the same time the Trust has a legal obligation to protect the confidentiality of its patients, whether they are in hospital or the community and whether they are alive or dead. Duty is breached where information about a patient is disclosed and this could be the simple acknowledgement that s/he is a patient of the Trust.

A request from the Police to access a person’s records should (where appropriate) be accompanied by the subject’s consent, see appendices for (request form) and will be processed in the same way as any other request received from a third party having patient consent.
However, there may be occasions where it is not possible, or may be inappropriate, to obtain consent. e.g. the service user themselves may be under investigation for a serious crime when asking for consent might jeopardise the police investigation or the patient or others are observed by the police to be at serious risk of harm and consent from the service user cannot be reasonably sought. The circumstances where this can arise are diverse and need to be considered on an individual case-by-case basis. They can include circumstances where a patient or former patient is the victim of a crime or is suspected of having committed an offence.

The Police have powers in such circumstances as described in the above paragraph to provide, under the Data Protection Act, a Section 29(3) form. This must be signed by a senior officer (inspector or above) and contain justification acceptable to the Trust of why patient information should be disclosed without their consent. The Trust will normally but are not compelled to, comply with such requests in the public interest.

13.4.1 Urgent Police Requests
Where there is a serious risk to life, the police will normally contact the relevant team direct to obtain the information they require. The relevant Service Manager will be involved in this process. Any information provided must be followed up by written confirmation of what information was provided and why it was needed. This must be documented on the patients records on Amigos and the medical records team notified.

Anyone presenting to the Trust and claiming to be a police officer should be asked to produce their Warrant Card. This should apply to uniformed and non-uniformed officers.

The Subject Access Officer should be notified of, log and process police requests received from the police and the appropriate health professional made aware of the request. The request will normally be complied having taken all factors into account. If insufficient information has been provided, further clarification may be sought before disclosing information.

Individuals contacting the Trust by telephone and claiming to be a police officer should NOT be given information over the Telephone. Instead they should be asked to provide their telephone number along with their name, rank and number. This information should then be verified by contacting the appropriate Police service. Following verification of all the officers details, including their telephone number, you should then contact them on the number they provided.

If the consent of the patient cannot be obtained then the following principles apply:

i) The police do not have a general right of access to records or information about patients. Unless there is a court order, the final decision about what may be disclosed will rest with the Trust. However, any request for information by the police should be considered by the health professional who is in charge or was in charge of the patient's treatment in the first instance.

ii) Disclosure of confidential information may be necessary for the prevention or detection of serious crime. If therefore, a police officer is investigating a “serious indictable offence” the health professional in charge of the patient’s care should bear this in mind when deciding whether or not to disclose confidential information. The meaning of the term “serious indictable offence” is set out in the appendices.
iii) A police officer requesting disclosure of confidential information relating to a patient should be asked to provide:

- a. Confirmation that the offence being investigated is a serious arrestable offence;
- b. Why it is believed the subject of the request has committed or is about to commit such an offence;
- c. The reason it is believed the provision of the information requested will assist the investigation;
- d. A Certificate as shown at appendices should be completed by an officer not below the rank of Inspector and kept by the Data Protection Officer;
- e. Only information that is relevant to the police enquiry should be given. Initially this should be restricted to the name and address of the patient, but at the discretion of the person deciding on its release, may include additional details if they are relevant to the investigation;
- f. If the health professional in charge of the patient’s treatment decides against releasing information then the matter should be referred to the Caldicott Guardian for further consideration. The Caldicott Guardian will normally consult with the health professional in charge of the patient’s treatment before a decision is made whether or not to release the information.

13.5 Legal Guardian, Official Solicitor, Nearest Relative Or Partner

Legal Guardians or the Official Solicitor are occasionally appointed by the courts to look after the affairs of individuals where they are deemed not to have capacity to look after their own affairs. Information should only be provided to such individuals on production of their written request, which should be accompanied by a copy of their authority granted by the court. The same applies to nearest relatives or partners requesting information about a patient.

13.6 Hospital Chaplains

Hospital Chaplains form an important part of any NHS Trust providing patient care and are generally not afforded patient information, as they are currently not deemed to be Health Care Professionals with a “need to know”. Independent legal advice has been sought which indicates that the Trust may pass details to Hospital Chaplains about current In-patients within the Trust who are members of the same faith as the Hospital Chaplain, providing the patient has given their consent to the information being used in such a way. Where patients are treated by the Trust they should be asked either in out-patients or on admission as an in-patient if they consent to their name being passed to their denominational Hospital Chaplain(s) for purposes of visiting and providing spiritual care.

13.7 Requests for Access to the Records of a Deceased Person

Access to the Health Records of a deceased person comes under the Access to Health Records Act 1990 (c.23) Section 3(1)(f), subject to Section 4(3) & Section 5(2) of the Act.

This states that where the patient has died, the patient’s personal representative, i.e. executor, administrator or any person who may have a claim arising out of the patient’s death, may make an application for access to the relevant part of the deceased’s health record, to the holder of the record.

However, this is not a general right of access, it is a restricted right and the following circumstances could limit the applicant’s access:
a) if there is evidence that the deceased did not wish for any or part of their information to be disclosed; or
b) if disclosure of the information would cause serious harm to the physical or mental health of any person; or
c) if disclosure would identify a third party (i.e. not the patient nor a healthcare professional) who has not consented to that disclosure.

This process is to be completed by the legal representative of the deceased, i.e. the Executor or Administrator of the deceased’s estate and will be dealt with as requests made under DPA 1998.

As with the Data Protection Act, a health professional will be required to screen the notes before release.

13.8 Documenting the Request
A request for disclosure of information, and any decision to disclose such information, should be recorded in the patient’s clinical notes including to whom the information has been disclosed and when.

14. When Access May Be Refused

Access can be refused if the Trust has previously complied with an identical or similar request in relation to the same individual, unless a reasonable interval has elapsed between compliance with the one and receipt of the other.

In deciding what amounts to a reasonable interval the following factors should be considered: the nature of the information, the purpose for which the information is processed and the frequency with which the information is altered.

The Trust is not required to respond unless it is provided with sufficient details to enable it to locate the information and satisfy itself as to to the identify of the individual making the request along with any required fee.

There are a number of other instances when the Trust may refuse access:

I) The Data Protection (Subject Access Modification) (Social Work) Order 2000: (Order 415)² this provides that personal data held for the purposes of Social Work are exempt from the subject access provisions, where the disclosure to the data subject would be likely to prejudice the carrying out of Social Work, by causing serious harm to the physical or mental health, or condition, of the data subject, or another person.

In making decisions on whether or not to give access to certain information there is no general test of what constitutes a risk of serious harm. Decisions have to be made on a case by case basis. Restriction on the right of access should be exceptional and confined to serious harm, for instance where there is sufficient risk to the safety of a child for a child protection plan to be in place and where disclosure would prejudice the plan. In some cases, access may have to be denied permanently. In others it may have to be deferred. The person seeking access may need special counselling during the period of deferment.

The Order also provides that access cannot be refused on the grounds that another person would be identified where that person is a relevant person (e.g. Social
Worker) unless the serious harm test applies. In all cases where this exemption applies the subject need only be informed that data about him/her are being processed.

II) The Data Protection (Subject Access Modification) (Health) Order 2000: provides that the Trust must not disclose information about physical or mental health or condition without first consulting an “appropriate health professional” (as defined in the Order). This would normally be the person responsible for the data subject’s current clinical care in connection with the matters to which the information relates. This might, for example, be a GP or consultant psychiatrist.

III) The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000: [The Data Protection (Miscellaneous Subject Access Exemptions) (Amended) Order 2000] where other enactments themselves prevent disclosure, then a data subject cannot rely on the DPA to seek access to records. These include, for example, adoption records and reports, and parental order records and reports under section 30 of the Human Fertilisation and Embryology Act 1990.

15. **Where The Trust Decides To Refuse Access**

Any notification of refusal to disclose personal data should be given as soon as practicable and in writing, even if the decision has also been given verbally. The Trust should record the reasons for its decision and explain these to the data subject.

If the Trust decides not to disclose some or all of the personal information, when explaining their reasons to the applicant, they should distinguish between reliance on an exemption, and failure or inability to obtain the consent of another person whose identity would be disclosed, or such a person’s refusal to consent and the reason for such refusal.

In the event of the Trust refusing access to an individual’s records they may, if they so wish, take up the matter with the Information Commissioner. The Information Commissioner may be contacted using any of the following methods;

**POST:** Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

**TELEPHONE:** 01625 545745

**FACSIMILE:** 01625 524510

**E-MAIL:** mail@ico.gsi.gov.uk

16. **Maintaining A Record Of Access Requests**

The Trust should keep a permanent record of all Access Requests at each site receiving the request. Such a record may be paper based or electronic in the form of a database (the recording mechanism implemented is down to each individual site). It is important that all requests for access to records are NOT filed within a data subject’s medical records as such information is not to be used for clinical work and may prejudice the care of a service user.
The minimum data sets that should be recorded are;

1. Name of Service User
2. Date of Birth of Service User
3. NHS Number
4. Date of Death of Service User (if applicable)
5. Type of Records Requested (Psychiatric Casenotes/Computer Records/Social Care Records, Staff Records etc.)
6. Service Users Casenote Number(s)
7. Name or person or Organisation making request
8. Date Request received
9. Fee Payable
10. Date Fee Received
11. Date Information was made available to service user or nominated person
12. Any information withheld from the patient and reason
13. Who made the decision to withhold the information
14. Type of Access Granted (Unlimited/Restricted/Denied)

17.1 Monitoring Of Access Requests
Monitoring will be undertaken on a regular basis and Monitoring Returns must be made by staff dealing with “Access Requests” by completing “Form D” (Appendix A), and must be made to Trust Headquarters no later than the tenth day of each calendar month. The information contained within the returns must include details of all Access Requests made in the previous calendar month, i.e. the March Return must include details of all Access requests made to that site in February.

17. Procedure for Dealing With Subject Access Requests

Any request must be received in writing to the appropriate manager. If these are received in the teams and department they should be forwarded immediately to the Subject Access Officer.

If the data subject wishes to complete the application form, then this should be forwarded or sent to the Subject Access Officer.

- North Locality Medico. Legal Officer Park House NMGH
- South Locality Medico. Legal Officer Laureate House
- Central locality Medico. Legal Officer Park House NMGH
- Staff Records) - HR Department Chorlton House
- HMP Manchester Health of Healthcare HMP Manchester
- Trust Data Protection Officer - Head of Information Governance and Records Chorlton House

Any request, which is directed, to Manchester Mental Health and Social Care Trust HQ will be forwarded immediately to the relevant officer above.

If the request is from a solicitor in relation to a pre-action protocol, then a copy of the letter should be forwarded immediately to Corporate Services Manager at Trust HQ.

The request must be acknowledged within 7 working days of receipt, in writing. Attached are sample letters in the appendices.
Applicants making verbal requests should be asked to contact the relevant site above to obtain the necessary form. Form A(1)

The Subject Access Officer will:

a) Acknowledge receipt (Letter 1) of a letter/verbal request and send an appropriate application form for completion, where necessary. Form A(1)
b) Will create a document wallet in order to keep all correspondence and attach a log sheet (form F)
c) Check the completed application form for validity on its receipt or return. (Form) If proof of identity is not received request this using Letter 2.
d) Maintain a log sheet of all dates relevant to the process of each request.
e) Request further information from the client, if necessary, in order to validate the form. Letter
f) After validation will send a copy of the completed request to the appropriate Health Professional and by means of Form x which will ask if any of the exemptions outlined in the Act apply.

The Health Professional, before the patient’s health records are released to the patient or their authorised representative, must check the records to ensure that their release will not cause either or both of the following:

a) serious harm to the physical or mental health or condition of the patient or any other person by disclosure of the information or
b) where access would disclose information relating to or provided by a third person who has not consented to disclosure. (This does not include entries by a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient.)

By completion of the boxes on Form C, the health professional will indicate to the whether or not the patient/patient’s representative is allowed to see all or part of the record. The form should be signed, dated and immediately returned to the Subject Access Officer

Any correspondence between the health professional and client, relating to an Access Request should be copied to the Subject Access Officer.

The health professional who is currently or was most recently responsible for the clinical care of the data subject in connection with matters to which the information requested relates or, where there is more than one such health professional, the one who is the most suitable to advise on matters to which the information requested relates should sign the request off.

Where there is no health professional available then it will be the health professional who has the necessary experience and qualification to advise on matters to which the information requested relates. This will be the Lead Consultant for the service the patient is or was last under or the Medical Director.

The declaration form is to ensure the Trust has taken all reasonable steps to confirm the identify of the individual making the request or to confirm the applicant has the authority to make a request on behalf of the person whose records are being requested.

It is possible that a request for access on behalf of a data subject will include a consent form already. If the Trust is satisfied that this does confirm the applicant has the authority to act on behalf of the service user and enough details about which part of the notes are required, then the declaration and consent forms need not be used.
• If it is not clear from the written request what information is required the user/requester is asked to provide more specific details on the declaration form.

• Service Users should be given the opportunity to meet with their key worker/clinician for counselling prior to being provided access to their records.

• Service Users should also be given the opportunity to view their records with their care worker/clinician. Before doing so third party information should be removed from the file and proof of identity of the service user should be seen before granting access.

• The Subject Access Request Under the Data Protection Act 1998 form (Form the professional for completion to be returned within 7 days. If the professional responsible for the service user is no longer with the organisation then authorisation should be given by the clinician who has taken over the original consultant’s caseload or the relevant lead clinician.

• On receipt of the signed declaration form from the applicant, a second letter should be sent to the applicant notifying them of the charge payable if any. When subject access requests are made the Trust should take into account the applicant’s ability to pay or other circumstances and if appropriate should waive the fee.

Where an access request has previously been complied with, the Act permits that you do not have to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance. In view of this, a note of the fact that the client has had copies of his/her record at a particular date should always be included in the health record case note on completion of the process.

• On receipt of the fee, copies of the appropriate documents should be forwarded to the applicant or their representative within 21 days.

• If access is refused or limited an explanation must be given to the applicant and it is recommended that this be done face-to-face followed up by a written explanation.

• Fees and cheques should be paid to Manchester Mental Health and Social Care Trust.

17.2 Requesting, Receiving and Banking fees
In regard to charges levied for the access to records process, the following options for banking money collected apply. Please note that in all cases Financial Codes must be provided for the fee to be credited. It is important to quote the name and reference of the Solicitors, (if applicable), on the invoice request form (appendices).

When requesting payment an invoice request form, must be completed and sent to the requestor and a copy to the Finance Team at Trust HQ

Any cheques received should be made payable “Manchester Mental Health and Social Care Trust and sent to the relevant site as detailed above. The cheque(s) will be banked by the cashing staff by their usual process of banking.

Payment to be made by Cheque in all cases.

3 Ideally two forms of identification should be asked for. The forms of Identification should be one photographic piece of identification along with a recent Utility Bill bearing the individual’s name and current address should be asked for. Identification such as a Utility Bill should always be checked against AMIGOS for the current registered postal addresses of the client.
17.3 Amendments to Records
Patient records should reflect the observations, judgements and factual information collected by the contributing health professional. General Medical Council guidance states that health records should be clear, accurate and contemporaneous.

The Data Protection Act fourth principle also states that information should be accurate and kept up-to-date and this provides the legal basis for enforcing corrections when appropriate. However, an opinion or judgement recorded by a health professional, whether accurate or not should not be amended subsequently. Retaining relevant information is essential for understanding the clinical decisions that were made and to audit the quality of care.

If a data subject feels that information recorded on their record is incorrect then they should firstly make an informal approach to the health professional concerned or in the case of staff to their manager to discuss the situation with regard to the possibility of having the records amended.

Factual inaccuracies should be amended and a note made on the record to explain this.

If the data subject is still not satisfied it is good practice for data controllers to allow to include a statement within their record that they disagree with the content.

Further information regarding this is contained in the Service User Record Management Procedure

17.4 Dealing with Complaints
If a data subject is unhappy with the outcome of their access request; such examples may include, information withheld from them, or they feel their information has been recorded incorrectly within their health record; in order to help rectify the complaint, the patient should be encouraged to go through the following channels:

The health professional may wish to have an informal meeting with the individual in the hope of resolving the complaint locally. If the health professional feels that they cannot do anything for the patient locally, the patient should be advised to make a complaint through the Trust’s Complaints office, Chorlton House, 50 Manchester Road, Chorlton cum Hardy, Manchester M21 9UN

Ultimately, the patient may wish to take their complaint direct to the Information Commissioner.

Alternatively, if the patient wishes to do so, they may wish to seek legal independent advice to pursue their complaint.

18 Appendices - Appendices to this document can be found on the intranet under “Our Documents/Forms” as individual documents

18.1 Forms

- Form A(1) – Subject Access Request Form
- Form B – Identity Verification form
- Form C – Authorisation Form
- Form D - Invoice request form
• Form E – Police Request form – consent for release of medical records
• Form F - Serious offences list to be uploaded to intranet
• Form G – Log sheet -
• Form - Trust Approved Abbreviations list to be added

18.2 Letters

 Letter 1 – Acknowledgement letter
 Letter 2 – Obtaining proof of identity letter
 Letter 3 – Seeking further information
 Letter 4 – Seeking further information and proof of identity
 Letter 5 – Letter to Court Judge