### POLICY FOR MANAGING SUBJECT ACCESS REQUESTS

<table>
<thead>
<tr>
<th>REFERENCE NUMBER:</th>
<th>IM&amp;T/02</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION:</td>
<td>1</td>
</tr>
<tr>
<td>STATUS:</td>
<td>Approved</td>
</tr>
<tr>
<td>ACCOUNTABLE DIRECTOR:</td>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>AUTHOR:</td>
<td>Information Governance Manager</td>
</tr>
<tr>
<td>DATE OF LAST REVIEW/ORIGIN DATE:</td>
<td>February 2009</td>
</tr>
<tr>
<td>DATE OF THIS REVIEW:</td>
<td>N/A/May 2013/ October 2013/ January 2014/December 2014</td>
</tr>
<tr>
<td>APPROVED BY:</td>
<td></td>
</tr>
<tr>
<td>DATE OF APPROVAL:</td>
<td>May 2011</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>May 2009</td>
</tr>
<tr>
<td>DATE NEXT REVIEW DUE:</td>
<td>February 2015</td>
</tr>
<tr>
<td>REVIEW BODY:</td>
<td>Information Governance Steering Committee/ Human Resources/ Recruitment</td>
</tr>
<tr>
<td>CATEGORISATION:</td>
<td>Information Technology</td>
</tr>
<tr>
<td>DATE OF EQUALITY IMPACT ASSESSMENT:</td>
<td>May 2009</td>
</tr>
<tr>
<td>APPLICATION:</td>
<td>Trust wide</td>
</tr>
</tbody>
</table>
Policy for Managing Subject Access Requests

Contents page

1. Introduction .................................................................................................................. 3
2. Objectives ................................................................................................................... 4
3. Scope ............................................................................................................................ 4
4. Definitions / Abbreviations ......................................................................................... 5
5. Roles and responsibilities ......................................................................................... 5
6. Body of the policy ....................................................................................................... 5
6.9. Logging Subject Access Requests ........................................................................... 6
6.10. Importance Guidance Relating To Disclosure of Third Party Information ....... 7
6.11. Recruitment Records ............................................................................................ 7
6.13. Freedom of Information Request ......................................................................... 8
6.15. Request for Staff Records ..................................................................................... 8
6.16. Requests for Records Relating to the Recruitment Process .................................. 8
6.17. Police Requests, Court Orders related to patient/ staff member ....................... 9
6.18. Charges .................................................................................................................. 9
7. Equality ...................................................................................................................... 10
8. Review ....................................................................................................................... 10
9. Training and awareness ............................................................................................. 10
10. Monitoring ............................................................................................................... 11
11. Discipline ............................................................................................................... 11
12. Appendices – Subject Access Log .......................................................................... 13
13. Further enquiries, advice, complaints ...................................................................... 13
1. Introduction

1.1. The policy is required to provide consistency and compliance relating to the handling of subject access requests received into the organisation. To ensure compliance with the Data Protection Act 1998 legal requirements to process the request and provide a response to the data subject within 40 days of receipt of the request.

1.2. The Act allows individuals to find out what personal information is held about them by raising a subject access request with an organisation who holds the personal related data. This covers information held electronically and in some paper records. However, the information must demonstrate that it is structured information that is being requested by the individual. E.g. data is held in an electronic or manual filing system.

1.3. The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

1.4. The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

1.5. The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

1.6. Should an individual or organisation feel they're being denied access to personal information they're entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

1.7. The Data Protection Act covers computer records and some manual records. Most computer records can easily be found about a particular person and should be disclosed removing any third party information unless consent can be obtained from the third party. Manual records need to be in a relevant filing system. The files which form part of the relevant filing
system are structured or referenced in such a way that information about the applicant can be easily located. Where manual files fall within the definition of a relevant filing system, the content will either be sub-divided, which allows the searcher to go straight to the correct category and retrieve the information requested without a manual search, or will be indexed to allow the searcher to go directly to a relevant page(s).

1.8. For example, a set of legal files containing files divided into sections for legal aid, pleadings, orders, correspondence by year, instructions to counsel, counsel’s advice, will not be a relevant filing system because the divisions/referencing do not assist a searcher in retrieving the required personal information without the need to leaf through the file contents.

2. Objectives

2.1. To ensure compliance with subject access request raised by a data subject; through right of access to the data subjects own personal data; relating to structured information held in computerised or manual form by the organisation, which is enforced through the Data Protection Act 1998.

2.2. To ensure requests raised via a Data Protection Act subject access request are responded to within 40 days.

2.3. To ensure a consistent approach to the receipt, handling, processing and response for subject access requests processed across various services within the Trust.

2.4. To ensure charging schemes are appropriate and legal.

2.5. To ensure the Trust is able to monitor compliance with subject access requests response timeframes.

2.6. To ensure the Trust have justified and legally applied exemptions to the release of personal data. That is if the data subject or representative acting with the consent of data subject’s access request; is blocked either fully or partially.

3. Scope

3.1. This policy applies to all Trust staff in all locations including temporary employees, locums, agency staff, contractors and visiting clinicians who receive, handle, process or respond to subject access requests.

3.2. The scope of this policy predominately covers all staff working within Medico Lego, Recruitment, Human Resources, Occupational Health, Line Managers and Information Governance.
3.3. However, any member of staff may receive a subject access request and will need to refer to this policy to ensure the request is appropriately directed to prevent delays in responding to the request within the 40 day timeframe.

4. Definitions / Abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGSC</td>
<td>Information Governance Steering Committee</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td>Subject Access Request</td>
<td>A legal right of access for a data subject to raise a request to obtain copies of personal data stored about them.</td>
</tr>
<tr>
<td>Data subject</td>
<td>The person about whom data is stored</td>
</tr>
<tr>
<td>Structure information</td>
<td>Information that has been ordered in a particular way enabling efficient retrieval.</td>
</tr>
</tbody>
</table>

5. Roles and Responsibilities

5.1. This policy applies to all staff that manage, process and respond to subject access requests raised under a subject access provision within the Data Protection Act 1998.

6. Body of the policy

6.1. This policy is intended to provide guidance for departments and services who receive requests for personal data. These requests may be from:
- a member of staff who wishes to access their personnel record;
- a patient who wishes to access or obtain copies of their medical record;
- a third party appointed by a data subject with their consent to access or obtain copies of their personal data on their behalf;
- or a request by Police or other government agencies to access personal data about individuals through application of certain exemptions within legislation.

6.2. For example, Police requests may be received to release certain personal information about a patient or staff member to prevent a crime. The request will require careful validation and may not always be fulfilled by the organisation if it is felt the information requested is excessive or unnecessary for the purpose for which the information has been requested.
Trust solicitors from time to time may assist with such decisions. Ultimately a declined request by a third party may result in issue of a Court Order which will then require the organisation to comply with the request.

6.3. All departments services identified in this policy who process Data Protection Requests are required to ensure the following information is logged with the Information Governance Manager/Data Protection Lead.

6.4. The role of the Data Protection Lead will involve ensuring all areas of the Trust who receive and process requests have access to DPA training, guidance and ensure that subject access requests are complied with within the 40 day period.

6.5. Where a subject access request is to be declined or partially declined reasons will need to be justified to the Information Governance Manager/Data Protection Lead. From time to time Trust Solicitors may be used to validate a legal justification for withholding such information although it is considered that such cases should be rare.

6.6. In all circumstances care should be taken to ensure subject access requests are complied with within 40 days. The Data Protection Act requires subject access requests to be complied within forty days and in exceptional circumstances if it is not possible to comply within this period then the applicant should be informed.

6.7. This policy enforces all areas identified as having responsibility for processing requests for personal data must log in the first instance: (Please note Access to Medical Records is already centrally managed, requests are logged and audited and are thus exempt from logging a subject access request as described in section 6.9 of this policy)

6.8. For further guidance on processing subject access requests refer to the ICO technical guidance documents available on the Intranet at www.ico.gov.uk

6.9. Logging Subject Access Requests

6.9.1. Any area responsible for processing subject access requests must have a system in place for recording receipt of requests and recording details of the response. Please use the Subject Access Log Form provided in the Appendix.

6.9.2. On receipt of the request the applicant should be informed. This is when the clock should start in terms of processing the request.

6.9.3. The Information Governance Manager/Data Protection Lead must be notified when the request is to be declined partially or completely; with reasons why the request is going to be declined. (Please note the
request must not be declined without first informing the Information Governance Manager/ Data Protection Lead). This is to prevent the data subject raising a complaint unnecessarily with the Information Commissioners Office.

6.10. Importance Guidance Relating To Disclosure of Third Party Information

6.10.1. Where information related to third parties exists this should be either removed completely or genuinely anonymised unless consent can be obtained from the third party to release. (For Medical Records refer to the Policy and Procedure for Patient Access To Health Records)

6.11. Recruitment Records

6.11.1. e.g. References that have been provided by a third party (referee) in confidence does not necessarily mean that it will remain in confidence if it is believed to be a justified or legal reason for access to that information by a data subject.

6.11.2. Where references are requested it is considered good practice by the Information Commissioners Office (ICO) to contact the referees and try an obtain consent. If objections are raised it must be considered if the reason for the objection is valid and lawful. It must be stressed that this is very subjective process and where doubt arises contact the Information Governance Manager for further advice and guidance.

6.11.3. From time to time the Trust solicitors may be consulted to offer legal guidance with difficult requests.


6.12.1. If you wish to make a subject access request for your medical records, please contact:

Medico Legal Department  
Sandwell & West Birmingham Hospitals  
Sandwell Hospital  
Lyndon  
West Bromwich  
B71 4HJ

Or

Medico Legal Department  
Sandwell & West Birmingham Hospitals  
City Hospital  
Dudley Road  
Birmingham  
B18 7QH
6.13. Freedom of Information Request

6.13.1. Freedom of Information Requests are centrally managed. The FOI Lead manages the request process from time of receipt to the disclosure or decline of the FOI request.

6.13.2. FOI Request must be responded to within 20 working days. An audit trail is maintained to show legal compliance with FOI legal timeframes and to document justification when a request has been fully or partially declined.

6.13.3. Requests should be directed to:

Freedom of Information Lead
The Trust Secretary
Sandwell & West Birmingham Hospitals
City Hospital
Dudley Road
Birmingham B18 7QH

Or; e-mail FOI.Requests@swbh.nhs.uk

6.13.4. Please note Section 40 of the FOIA sets out an exemption from the right to know if the information requested is personal information protected by the DPA. The section has a fairly complex structure and refers in detail to DPA provisions and concepts.


6.14.1. Requests should be directed to the Occupational Health Department. These records will be processed in line with the Data Protection 1998 and Health Records Act 1990.

Sandwell Occupational Health Service
30 Hallam Close
Hallam Street
B71 4HU

6.15. Request for Staff Records

6.15.1. Staff request for Personnel records or other related personal data held in databases within the Trust can be obtained by directing the request to the staff’s line manager.

6.16. Requests for Records Relating to the Recruitment Process
6.16.1. Information relating to recruitment for both successful and unsuccessful candidates should be directed to the Recruitment department.

Recruitment Department
Data Protection Lead
Sandwell and West Birmingham Hospitals Trust.
Sandwell Hospital
Lyndon
West Bromwich
B71 4HJ

6.17. Police Requests, Court Orders, National Archive Requests relating to the Trust’s preserved records and other requests made legitimately by other government agencies to release personal data related to patient/staff member.

6.17.1. Requests for patient personal data of this nature will be processed by Medico Legal Services in line with the Access to Health Records Policy.

6.17.2. Requests for staff personal data should be directed to the Trust’s Data Protection Lead who will processed in line with this policy:

Information Governance Manager
Data Protection Lead
Sandwell and West Birmingham Hospitals Trust.
Sandwell Hospital
Lyndon
West Bromwich
B71 4HJ

6.17.3. These types of requests will require validation to ensure they are legitimate. Requests of this nature will be assessed to ensure the requesting organisation is permitted by law to access the personal data requested and to ensure that the information is not excessive in the context of the purpose for which the request is required. This is a subjective process and from time to time Trust Solicitors will be accessed to provide legal guidance.

6.17.4. Where court orders are issued these must be complied with. However the court order should be validated to ensure it is legitimate.

6.18. Charges

6.18.1. There are different charges applicable depending on the type and format (computerised/manual) of personal data requested.
6.18.2. A fee may be payable. At the time of writing the maximum fee is £10. If information is held in both computer form and in structured paper files, a single £10 fee covers both.

6.18.3. Different rules apply to health and educational records, where a £50 charge could be applied (including the cost of all photocopies). For credit reference agency records the maximum fee is £2.

6.18.4. Example: one copy of information per request. Consecutive copies will each be processed and charged as a separate requests. This is to ensure all or part of the expense incurred by the organisation is recovered when producing the information in the required format.

7. **Equality**

7.1. The Trust recognises the diversity of the local community and those in its employ. Our aim is, therefore, to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. The Trust recognises that equality impacts on all aspects of its day-to-day operations and has produced and Equality Policy Statement to reflect this. All policies are assessed in accordance with the Equality initial screening toolkit, the results for which are monitored centrally.

8. **Review**

8.1. This policy will be reviewed in 2 years time. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation of guidance.

9. **Training and awareness**

9.1. There are various levels of training available to provide awareness of the Data Protection Act 1998.

9.2. For general awareness refer to the: Information Governance e-learning module available on the Trust Learning and Development Internet site or the Information Governance Workshop sessions which can be booked by contacting the Information Governance Manager.

9.3. Tailored sessions may also be booked by contacting the Trust Information Governance Manager.

9.4. There is also a Data Protection, British Computer Society (BCS) accredited course. The Data Protection BCS course is available from various BCS accredited training providers and test centres. Learners can select
appropriate in-depth modules or decide to complete the full Data Protection accreditation course.

10. **Monitoring**

10.1. It is critical that key personnel responsible for managing subject access requests or processing and responding to them do so in a timely manner and apply exemptions correctly on refusal to supply part or all of the information requested. This is to ensure legal compliance with subject access requests.

10.2. The Information Governance Manager/Data Protection Lead will require quarterly report detailing all non-health records requests received and processed within each quarter so that compliance with the agreed timescales can be monitored.

10.3. Compliance issues will be recorded on the corporate risk register and raised at the Information Governance Steering Committee who will seek appropriate action within the organisation by those accountable. Action plan will be created to address compliance issues.

11. **Discipline**

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

11.2. Subject access requests not responded to in line with legal requirements may reported to the Information Commissioner’s Office who enforce compliance with the Data Protection Act 1998 and Freedom of Information Act 2000. Organisations/individuals could be prosecuted or fined by the ICO for failure to comply.

12. **Bibliography**

12.1. Data Protection Good Practice Note Releasing information to prevent or detect crime

A quarterly update of this log must be sent to the Information Governance to provide internal assurances regarding legal compliance.

<table>
<thead>
<tr>
<th>Date Request Received?</th>
<th>Date Receipt Of Request Sent To Recipient?</th>
<th>Department/Service Who Received The Request?</th>
<th>Ref No Assigned By Department/Service?</th>
<th>Insert an Electronic Copy Of The Request?</th>
<th>Who Received The Request?</th>
<th>Who Is Assigned To Process The Request?</th>
<th>Date Request Was Responded To?</th>
<th>Exemption Applied Partially Or Fully? Please State Details</th>
<th>Total Number Of Days Taken To Respond To The Request?</th>
<th>Additional notes.</th>
</tr>
</thead>
</table>
14. **Further enquiries, advice, complaints**

14.1. For Data Protection Subject Access Requests Contact:

    Information Governance Manager  
    Data Protection Lead  
    Sandwell and West Birmingham Hospitals Trust.  
    Sandwell Hospital  
    Lyndon  
    West Bromwich  
    B71 4HJ

14.2. For Freedom of Information Requests Contact:

    Freedom of Information Lead  
    The Trust Secretary  
    Sandwell & West Birmingham Hospitals  
    City Hospital  
    Dudley Road  
    Birmingham B18 7QH