

Overarching protocol for information sharing in Ealing

To provide a framework for the sharing of information in Ealing between all partner organizations

September 2009



Contents

1. Preface	1
2. Introduction	2
3. Aims and objectives	3
4. Scope	4
5. Key principles	5
6. The legal framework	6
7. Purposes for sharing information	7
8. Use of anonymised information	8
9. Sharing information with the consent of the data subject	9
10. Sharing information without the consent of the data subject	10
11. Secondary disclosure	11
12. Access to information	12
13. Organisational responsibilities	13
14. Individual responsibilities	15
15. Complaints	16
16. Monitoring & reviewing arrangements	17
Appendices:	
Appendix A: signatures	18
Appendix B: the legal framework	19
Appendix C: information sharing agreement template	25
Appendix D: glossary of terms	28

1. Preface

1.1 This protocol has been jointly developed by public sector and 3rd Sector organisations operating in Ealing to facilitate the sharing of information between them so that members of the public receive the services they need.

1.2 Extensive consultation has taken place within each of the agencies that are party to this protocol. This protocol has been presented to the relevant management boards within each agency.

Ealing

2. Introduction

2.1 This protocol sets out the principles for using and sharing personal information among the partner organisations listed in appendix A who operate in Ealing.

2.2 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. *The balance between the need to share information to provide quality services and to facilitate accurate monitoring and the protection of confidentiality can be a difficult one to achieve.*

2.3 Uncertainty over the legal position may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly and provide the services required.

Ealing

3. Aims and objectives

- 3.1 The overall aim of this protocol is to provide a framework for the partner organisations to establish and regulate working practices in order to ensure that information is managed and shared on a lawful, 'need to know' basis.
- 3.2 The main objectives are:
 - a. to increase awareness and understanding of the relevant legislation and especially the Data Protection Act 1998;
 - b. to guide partner organisations on how to share personal information lawfully;
 - c. to promote the development and use of Information Sharing Agreements;
 - d. to encourage lawful flows of information; and
 - e. to support a process, which will monitor and review information flows.
- 3.3 This protocol will be used in conjunction with local service level agreements, contracts or any other formal agreements that already exist between the partner organisations.

4. Scope

- 4.1 This protocol sets out the principles that all partner organisations will follow when using and sharing personal information.
- 4.2 In this protocol the terms 'data' and 'information' are synonymous.
- 4.3 The protocol applies to all personal information¹ handled by the partner organisations including information held on manual records and information processed electronically by computer, CCTV or audio recordings.
- 4.4 The Data Protection Act also defines certain classes of personal information as 'sensitive data'² where additional conditions must be met for that information to be used and disclosed lawfully.
- 4.5 Personal data ceases to be so when a data subject can no longer be identified from the data. Such data is not subject to the Data Protection Act 1998.

¹ 'Personal information' is data relating to a living individual who can be identified from that data or by other data which is in the possession of or likely to come into the possession of the partner organisation

² 'Sensitive data is information as to racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or mental health, sexual life, commission or alleged commission of an offence, criminal proceedings or sentence'

5. Key principles

The partner organisations agree:

- 5.1 to share information with each other where it is lawful to do so;
- 5.2 to comply with the requirements of the Data Protection Act 1998 and in particular with the 8 Data Protection Principles (see appendix B);
- 5.3 to inform data subjects when and how information is recorded about them and how their information may be used;
- 5.4 to ensure that adequate security measures are applied to the personal data they hold and transfer and commit to comply as far as possible with SO1799/BS7799³;
- 5.5 to have due regard to the guidance published by the Information Commissioner to help those in the public sector comply with the Data Protection Act. (See www.informationcommissioner.gov.uk);
- 5.6 to develop local Information Sharing Agreements that govern the way transactions are undertaken between the partner organisations and with other organisations that are not parties to this protocol. (See appendix C for template);
- 5.7 to promote staff awareness of the protocol and to train staff in the principles of lawful information sharing; and
- 5.8.1 to promote public awareness of the need for information sharing through the use of appropriate communications media including publishing the protocol on the websites of the respective agencies.

³ BS77993 is the most widely recognised security standard in the world. It is comprehensive in its coverage of security issues, containing 127 control requirements, structured under 10 major headings such as Personnel Security, Access Controls and Security Organisation.

6. The legal framework

- 6.1.1 In general, people have a right to choose how their personal data is used and who may have access to it. However the law allows for information to be shared where there is a legitimate purpose and a legal basis.
- 6.1.2 Public bodies require administrative powers to share information for specific purposes and these powers will often be provided by a statutory provision which sets out the lawful basis for disclosure.
- 6.1.3 The principal laws concerning the protection and use of personal information are listed below and further explained in appendix B:
 - >> the Data Protection Act 1998
 - >> the Human Rights Act 1998 (article 8)
 - >> the Freedom of Information Act 2000
 - >> the Common Law Duty of Confidence
 - >> the Caldicott Principles

7. Purposes for sharing information

- 7.1 The partner organisations will clearly identify the specific purposes for which they may need to share information. These will be recorded in Information Sharing Agreements.
- 7.2 The partner organisations will ensure that the Information Commissioner has been notified of the purposes for which they share information.
- 7.3 The partner organisations will ensure where appropriate that data subjects are provided with a 'Fair Collection Notice'⁴ at the time they provide personal information. This will state the identity of the data controller, the purposes(s) for which the data are intended to be processed and the organisations with whom it may be shared. If the Data Controller has a nominated representative for the purposes of the Data Protection Act, the identity of that representative should be provided.
- 7.4 The partner organisations will also ensure that this information for data subjects is made readily and easily available through websites and leaflets to those about whom personal data is already held.
- 7.5 The partner organisations will ensure that information is requested and shared on the principle that it will be made available only on a justifiable 'need to know basis'. This means that staff will have access to information only if the function they are required to fulfill in relation to a particular service user cannot be achieved without access to the information in question.

⁴ Schedule 1: Part 11(2) and (3) Data Protection Act 1998

8. Use of anonymised information

- 8.1 Information will be anonymised before it is shared wherever that is possible and practicable.
- 8.2 It is important that care is taken to ensure that anonymised data, especially when combined with other information from different agencies, does not identify an individual either directly or indirectly and the data cannot be combined with any data sources held by a partner to produce personal identifiable data.

9. Sharing information with the consent of the data subject

- 9.1 Where possible partner organisations will seek consent from a service user before sharing his/her personal information with other partner organisations.
- 9.2 Where consent to disclose information is requested the service user will be made aware of the information it is proposed to share and the purposes for which it will be used.
- 9.3 The partner organisations will ensure that where it is given consent *it* is given freely and constitutes informed consent. In the case of 'sensitive personal data', where it is obtained consent will always be explicit and obtained specifically in relation to the proposed processing of the data.
- 9.4 The data subject will have the right to withdraw consent at any time and should be informed of this right
- 9.5 The partner organisations will agree standards and procedures for ensuring that a written record is kept of consent given or withdrawn.
- 9.6 The partner organisations will also agree specific procedures, which will apply where the data subject is either under the age of 16 or where the data subject does not have the capacity to give informed consent or when it is not reasonably practical to obtain consent. These will be recorded in the relevant Information Sharing Agreement.

10. Sharing information without the consent of the data subject

- 10.1 There are circumstances when it is lawful to disclose personal information about an individual without their consent.
- 10.2 The Data Protection Act recognises that in certain circumstances the public interest requires the disclosure of personal data disclosure of which might otherwise be in breach of the Act and creates certain exemptions from the non-disclosure provisions. For example, the exemptions include disclosures required by law or in connection with legal proceedings and for the prevention or detection of crime or where necessary to protect the vital interests of the data subject.
- 10.3 In addition the Data Protection Act 1998 permits the processing of personal information and sensitive personal information if the processing satisfies certain conditions. These conditions are set out in Schedules 2 and 3 of the Act. (See www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10#sch2)
- 10.4 The conditions include, but are not limited to, processing with consent.
- 10.5 The conditions which are most likely to be relevant where personal information is shared is that the disclosure is necessary for the exercise of a statutory function of one or more of the public bodies; that the processing is necessary to protect the vital interest of the data subject or the processing is necessary for the exercise of any other functions of a public nature exercised in the public interest.
- 10.6 When relying on these conditions it is still important to consider the rights of the data subject to confidentiality and to ensure that information is only shared where there is a justifiable need to do so.
- 10.8 Decisions to disclose or to decline to disclose information without consent will be made by an authorised officer and recorded for audit purposes. The partner organisations will keep an up to date list of authorising officers and their contact details.

11. Secondary disclosure of information to other partners and agencies who are not signatories of the protocol

11.1 Subject to para 11.3 below, secondary disclosure will not be made without the consent of the originating partner unless:

it is recorded in an Information Sharing Agreement to which the originating partner is a signatory that the information can be shared without the permission of that originating partner

11.2 Any such agreement or disclosure will be based on the following principles:

- the necessary condition(s) in Schedule 2 and 3 Data Protection Act 1998 are satisfied;
- there is a justifiable need for the disclosure to take place; and
- the partner organisation making the secondary disclosure is satisfied that adequate security arrangements are in place as a result of the existence of an Information Sharing Agreement with the third agency.

11.3 Secondary disclosure may be made without the consent of the originating agency if ordered by the court. In this case the disclosing agency will notify the originating agency of its actions.

12. Access to information

- 12.1 The partner organisations will maintain accurate records and will inform data subjects of their procedures for seeking access to information held about them.
- 12.2 The partner agencies will develop systems to record consent given or refused, the sharing or transfer of information and deletion of and/or amendment to data held.
- 12.3 Where rectification or deletion of data held by one of the partner agencies occurs, whether at the request of the data subject or otherwise, any changes made as a result will be recorded and communicated to all organisations with whom the data had previously been shared.

13. Organisational responsibilities

- 13.1 Each partner organisation is responsible for ensuring that personal data passed to them is clearly marked and kept securely within a passworded computer system or otherwise physically secure with appropriate levels of staff access.
- 13.2 Partner organisations will accept the access levels on supplied information and handle the information accordingly.
- 13.3 Partner organisations accept responsibility for independently or jointly auditing compliance with the Information Sharing Agreements in which they are involved *at least annually*.
- 13.4 Partner organisations will take steps to ensure that their staff are aware of their responsibilities under the Data protection Act to ensure compliance with the Act. Relevant staff will be provided with copies of Information Sharing Agreements which cover services they provide.
- 13.5 Every organisation will make it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of confidential information.
- 13.6 Any failure by an individual to follow the policy will be dealt with in accordance with that organisation's disciplinary procedures.
- 13.7 Every partner organisation will ensure that procedures are in place to ensure that disclosure of information without the consent of the data subject or secondary disclosure will only occur after authorisation by an appropriate officer. An up to date list of authorising officers and their contact details will be kept by each of the partner organisations.
- 13.8 The partner organisations supplying information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information as soon as it has been identified. These breaches will be recorded and partner organisations will investigate and report back to the information manager/data protection officer.
- 13.9 Partner organisations will have documented policies for retention, weeding and secure waste destruction and they will be available for inspection by all partner organisations.
- 13.10 Each statutory partner organisation will ensure that a suitably senior officer is designated to represent the organisation on a steering group, chaired by the Head of the Information Management Group of Ealing Council, which will oversee the implementation, monitoring, and review of the protocol. This officer will ensure that their contact details are passed to all partner agencies. 3rd Sector

organisations will elect 2 officers to sit on the group and to report back to other organisations.

- 13.11 The Information Sharing Agreements will specify data to be shared and the timing for the production of this data. Partner organisations should give at least 3 months notice when changing the details if these agreements.

14. Individual responsibilities

- 14.1 Every individual working for the organisations listed in this protocol is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.
- 14.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.
- 14.3 Every individual has an obligation to request proof of identity, or take steps to validate the authorisation of another before disclosing any information.
- 14.4 Every individual should uphold the general principles of confidentiality, follow the rules laid down in this protocol and seek advice when necessary.
- 14.5 Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal.

15. Complaints

- 15.1 Complaints about the use of personal information will be dealt with under the relevant complaints procedure of the partner organisation whose actions are the subject of complaint. The partner organisations agree to cooperate in any complaint investigation where they have information that is relevant to the investigation. If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers who should liaise to investigate the complaint.
- 15.2 The partner organisations will notify the Head of the Information Management Group at Ealing Council of any complaints and the outcome of any complaint investigation.

16. Monitoring & reviewing arrangements

- 16.1 Partner organisations will take individual responsibility for monitoring and reviewing the implementation of the protocol and the use of Information Sharing Agreements in their organisation.
- 16.2 The Information Manager of Ealing Council in conjunction with the partner agencies will formally review this overarching protocol annually unless new or revised legislation or national guidance necessitates an earlier review.
- 16.3 Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

Appendix A: Partners

- Ealing Council
- NHS Ealing
- Ealing Homes
- Ealing Hospital Trust
- West London Mental Health Trust
- Metropolitan Police
- London Fire Brigade
- Ealing Community Network (on behalf of the Voluntary and Community Sector in Ealing)

Appendix B: the legal framework

The Data Protection Act 1998

The Act governs the protection and use of personal data. Personal data means data relating to living individuals.

Any organisation processing (obtaining, holding, using, disclosing and disposing) data is a 'Data Controller' responsible for abiding by the 8 data protection principles and notifying the Information Commissioner of that processing.

The Act gives seven rights to individuals in respect of their own personal data:

1. right of subject access;
2. right to prevent processing likely to cause damage or distress;
3. right to prevent processing for the purposes of direct marketing;
4. rights in relation to automated decision taking;
5. right to take action for compensation if the individual suffers damage or damage and distress (as a result of any breach of the act);
6. right to take action to rectify, block, erase or destroy inaccurate data;
7. right to request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The 8 key principles of the Act are:

Principle 1	Personal data shall be processed fairly and lawfully and shall not be processed unless at least 1 of the conditions in Schedule 2 is met and for 'sensitive personal data' at least 1 of the conditions in Schedule 3 is also met.
Principle 2	Personal data shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.
Principle 3	Personal data shall be adequate, relevant and not excessive in relation to the purpose/purposes for which they are processed.
Principle 4	Personal Data shall be accurate and, where necessary kept up to date
Principle 5	Personal data shall not be kept for longer than is necessary for that purpose/purposes.
Principle 6	Personal data shall be processed in accordance with the rights of the data subject under this Act.
Principle 7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.
Principle 8	Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Schedule 2 and Schedule 3 conditions

Lawful processing of personal data requires that one condition in Schedule 2 should be met; and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Conditions in Schedule 2	
Paragraph 1	The data subject has given consent to the processing.
Paragraph 2	The processing is necessary for (a) the performance of any contract to which the data subject is a party; (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
Paragraph 3	The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
Paragraph 4	The processing is necessary in order to protect the vital interests of the data subject.
Paragraph 5	<p>The processing is necessary:</p> <p>(a) for the administration of justice;</p> <p>(b) for the exercise of any functions conferred on any person by or under any enactment;</p> <p>(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or</p> <p>(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.</p>
Paragraph 6	<p>(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.</p> <p>(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.</p>

Conditions in Schedule 3	
Paragraph 1	The data subject has given explicit consent to the processing.
Paragraph 2	The processing is necessary for the purposes of exercising or performing a legal right or obligation in the context of employment.
Paragraph 3	The processing is necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained.
Paragraph 4	The processing is of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit bodies.
Paragraph 5	The processing is of information made public as a result of steps deliberately taken by the data subject.
Paragraph 6	The processing is necessary in connection with legal proceedings or the seeking of legal advice.
Paragraph 7	The processing is necessary: (a) for the administration of justice; (b) for the exercise of any function conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
Paragraph 8	The processing is necessary for medical purposes and is carried out by medical professionals or others owing an obligation of confidence to the data subject.
Paragraph 9	The processing is necessary for ethnic monitoring purposes.
Paragraph 10	The personal data are processed in circumstances specified in an order made by the Secretary of State for certain purposes. The Data Protection (Processing of Personal Data) Order 2000 (SI 2000 No 417) specifies a number of circumstances in which sensitive personal data may be processed such as crime prevention, policing and regulatory functions (subject to a substantial public interest test); insurance, equality monitoring in the area of disability and religious or other beliefs; and research. A further order relates to the processing of sensitive personal data by MPs and other elected representatives (The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (SI 2002 2905)).

The Human Rights Act 1998

The Human Rights Act 1998 incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act places a legal obligation on all Public Authorities to act in a manner compatible with the Convention. Should a Public Authority fail to do this then it may be the subject of legal action. The sharing of information between agencies has the potential to infringe Article 8.1 in particular. Article 8.1 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This right may be only breached by a public authority if the breach is in accordance with the law and is necessary in the interest of one of the following legitimate aims: national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others.

The following factors should be taken into account when deciding whether disclosure of information would breach a person's right to privacy

- is there a legal basis for the action being taken?
- does it pursue a legitimate aim?
- is the action taken proportionate and the least intrusive method of achieving that aim?

The Freedom of Information Act (FOIA) 2000

The Freedom of Information Act (FOIA) gives a general right of access to the public of all types of recorded information held by defined public authorities from 1 January 2005.

There are 23 statutory exemptions to the right of access which are either absolute or qualified. Absolute exemptions include personal information if disclosure would breach the data protection principles. Qualified exemptions require the public authority to consider first whether or not the exemption applies, on a case-by-case basis. Secondly, if the exemption does apply, the public authority must then consider whether it is in the public interest to apply the exemption. Further information and guidance can be found at the following web site <http://www.informationcommissioner.gov.uk>

The Common Law Duty of Confidentiality

This duty arises where information has the necessary quality of privacy. Disclosure of that information without the consent of the individual could give rise to a civil claim for breach of the duty. However it would be a defence to such a claim to show that the breach of confidence was in the public interest and disclosure was to the extent necessary for the performance of a public duty.

Caldicott Principles

The Caldicott Committee carried out a review of the use of patient-identifiable information. It recommended a series of principles that should be applied when considering whether confidential information should be shared. All NHS organisations and Social Services Departments are now required to apply the Caldicott principles. These principles relate to the use of patient-identifiable information and are detailed below.

Principle 1	Justify the purpose for using such information. Every proposed use or transfer of such information should be clearly defined and scrutinised and continuing uses reviewed regularly.
Principle 2	Only use such information when absolutely necessary.
Principle 3	Use the minimum information that is required for a given function to be carried out
Principle 4	Access should be on a strict “need to know” basis. Only those staff who need such information in order to carry out their roles should have access and this should be limited to specifically relevant information.
Principle 5	Everyone with access to such information needs to be aware of their responsibilities and their obligations in respect of confidentiality.
Principle 6	Understand and comply with the law. Someone in each organisation that handles personally identifiable information should be responsible for ensuring that the organisation complies with legal requirements.

All Health and Social Services organisations are required to nominate a senior person to act as a Caldicott Guardian responsible for safeguarding the confidentiality of patient information.

Examples of Statutory Gateways for disclosure

i. Crime and Disorder Act 1998

The Act is concerned with measures to reduce crime and disorder. Section 115 provides that any person has the power to lawfully disclose information to the police, local authority, probation service or health authority where the disclosure is necessary or expedient for the purposes of any provision of the Act.

However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement to exchange information and does not override the need to disclose in a proper manner taking into account Data Protection Principles and Article 8 Human Rights Convention.

ii. Local Government Act 2000

Under Section 2 local authorities may do anything, which they consider likely to achieve any one or more of the following objects:

- the promotion or improvement of the economic well-being in their area;
- the promotion or improvement of the social well-being of their area; and
- the promotion or improvement of the environmental well being of their area.

The power may not be exercised where there is an express restriction on doing so.

iii. Criminal Justice and Court Services Act 2000

Section 67 of this Act establishes multi-agency arrangements for the assessing and managing the risk posed within their areas by sexual and violent offenders and other offenders considered to be potentially dangerous.

iv. Health and Social Care Act 2011 (Section 60)

Section 60 of the Act provides a power to ensure that patient-identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public where consent is not a practical alternative and where anonymised information will not suffice. It is intended largely as a transitional measure whilst consent or anonymisation procedures are developed which is reinforced by the need to review each use of the power annually.

The reason for this provision is mainly in relation to the carrying out of large-scale research projects, which may involve tens of thousands of patients where contact would be impracticable.

The essential nature of such research is put forward as the justification for the “public good” outweighing issues relating to privacy and confidentiality.

v. National Health Service Act 1977

Under Section 22 NHS bodies (on the one hand) and local authorities (on the other) shall co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.

National Health Service and Community Care Act 1990

Under Section 47 When a local authority is assessing need and it appears that there may be a need for health or housing provision, the local authority shall notify the appropriate primary care trust or local housing authority and invite them to assist to such extent as is reasonable in the circumstances in the making of the assessment.

vi. Children Act 1989

Sections 27 and 47 of the Children Act 1989 enable local authorities to request help from specified authorities (other local authorities, education authorities, housing

authorities, NHS bodies) and place an obligation on those authorities to co-operate. A request could be for information in connection with a s17 needs assessment or a s47 child protection enquiry.

vii. Children Act 2004

Section 10 (co-operation to improve well-being) and section 11 (arrangements to safeguard and promote welfare) brings with them an implied duty to share information when judged to be in the best interests of the child. That is, those bodies bound by the duties should share information about children as part of furthering those duties. The Children Act 2004, therefore, adds to and reinforces the existing body of legislation that gives (usually in an implied way) legal foundation to information sharing when the interests of a child require it.

viii. Education Act 2002

S175 (2) provides that the governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.

ix. Learning and Skills Act 2000

S117 places a duty on a range of educational establishments to provide information to Connexions for the purpose of provision of services to pupils unless the parents of a pupil under 16 or the pupil himself if over 16 has given instructions that information may not be provided.

Examples of statutory restrictions to information sharing

The NHS (Venereal Diseases) Regulations 1974 and **NHS Trusts (Venereal Diseases) Regulations 1991** prevent the disclosure of any identifying information about a patient with a venereal disease other than to a medical practitioner under specified circumstances.

The Human Fertilisation and Embryology Act 1990 (as amended) limits the circumstances in which information may be disclosed by centres licensed under the Act.

The Abortion Regulations 1991 limit and define the circumstances in which information submitted under the Act may be disclosed.

IF IT SEEMS LIKELY THAT INFORMATION TO BE SHARED FALLS INTO ONE OF THESE CATEGORIES FURTHER ADVICE SHOULD BE SOUGHT.

Appendix C: information sharing agreement template

This is an agreement between ORGANISATION 1 and ORGANISATION 2

It is made under the auspices of the Ealing Information Sharing Protocol.

1. PURPOSE OF THIS INFORMATION SHARING AGREEMENT

- ⌚ A clear statement of why there is a need to share information between the organisations party to this Information Sharing Agreement.
- ⌚ Reference should be made to the legislation which underpins the statutory functions for which information sharing is necessary and any Guidance that supports data sharing.

2. EXTENT AND TYPE OF INFORMATION TO BE SHARED

- ⌚ The data exchanged should be the minimum amount necessary for the performance of the relevant services. The agreement should clearly state what information is shared routinely.

3. HOW THE INFORMATION MAY BE USED

For example:

- a. Who will have access to the information within the parties to the ISA?
- b. What information is it necessary to share routinely?
- c. Who will authorise transfer of routinely shared information if the data subject has indicated that they do not agree to certain information being shared?
- d. How will the reasons for transfer in these circumstances be recorded?
- e. In what circumstances will explicit consent be sought to information being shared?
- f. In cases where explicit consent is sought how will the giving or withdrawal of consent to share information be recorded?
- g. How will the issue of consent be handled in respect of people under the age of 16 or adults who lack the capacity to give consent?
- h. In what circumstances can secondary disclosure beyond the partners to the ISA take place without the explicit permission of the originating organisation?

- i. Where the permission of the original provider of the information is required prior to secondary disclosure how will that permission be obtained and recorded?
- j. How long will the information be retained?
- k. What are the arrangements for secure storage and destruction of the information?
- l. What are the arrangements for subject access to the information?
- m. In what circumstances would it be reasonable for the data subject to be given access to their information without the specific consent of the original provider?
- n. Where the consent of the original provider is required before giving subject access how will it be obtained and recorded?
- o. What are the arrangements for rectifying errors in data

4. INFORMATION TO DATA SUBJECTS

- ⌚ What information are data subjects given about the purposes for which their information may be used, with whom it may be shared, how they can access it and rectify errors and how they might complain about the way their information has been used

5. BREACHES OF CONFIDENTIALITY

How are you going to deal with:

- ⌚ any breach of agreement by staff,
- ⌚ monitoring security incidents, and
- ⌚ complaints about data sharing which involve more than one agency and notification to the Head of the Information Management Group of Ealing Council

6. STAFF AWARENESS AND TRAINING

- ⌚ What are the arrangements for this?

7. GOVERNANCE

- I. Named individuals to lead on ISA
- II. Who will monitor compliance with the ISA

8. REVIEW OF INFORMATION SHARING AGREEMENT

- ⌚ How long will the ISA last
- ⌚ When will the ISA be reviewed

9. CLOSURE/TERMINATION OF AGREEMENT

- ⌚ What will happen if there is a serious breach of confidentiality?
- ⌚ How will the Partners be able to terminate the agreement?

10. SIGNATORIES

This agreement is signed on behalf of:

Name of organisation:

Name of officer:

Title:

Date:

Name of organisation:

Name of officer:

Title:

Date:

Appendix D: glossary of terms

ACCESSIBLE RECORD	Unstructured personal information usually in manual form relating to health, education, social work and housing.
CALDICOTT PRINCIPLES	A set of 18 standards established through the work of the government committee chaired by Dame Fiona Caldicott in 1996/1997 to establish clear standards for Information Security & confidentiality within the NHS.
CCTV	Close Circuit Television.
CONSENT	Any freely given, specific and informed indication of wishes which the data subject gives to signify their agreement to personal (and, where appropriate, sensitive personal) data relating to them being processed
DATA	<p>a) Information being processed by means of equipment operating automatically; or</p> <p>b) Information recorded with the intention it be processed by such equipment.; or</p> <p>c) Information recorded as part of a relevant filing system; or</p> <p>d) Information not in a, b or c, but forming part of an accessible record.</p>
DATA CONTROLLER	A person or a legal body such as a business or public authority who jointly or alone determines the purposes for which personal data is processed.
DATA SUBJECT	An individual who is the subject of personal information.
DISCLOSURE	The passing of information from the Data Controller to another organisation / individual.
DUTY OF CONFIDENTIALITY	Everyone has a duty under common law to safeguard personal information.
EUROPEAN ECONOMIC AREA (EEA)	This consists of the fifteen EU members together with Iceland, Liechtenstein and Norway.
FAIR COLLECTION NOTICE	To inform the data subject how their data is to be processed before processing occurs. Ensuring so far as practicable that the data subject has:
	<p>a) the identity of the data controller,</p> <p>b) the identity of any nominated representative for the purposes of the Data Protection Act,</p> <p>c) the purpose(s) for which the data is intended to be processed, and</p> <p>d) any further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed.</p>
INFORMATION	See 'DATA' above
INFORMATION SHARING AGREEMENT (ISA)	A specific agreement drawn up by two or more organisations that need to share personal information about service users. See appendix C.

NEED TO KNOW	To access and supply the minimum amount of information required for the defined purpose. A service or organisation signed up to the protocol
<i>PARTNER ORGANISATION</i>	
<i>PERSONAL DATA</i>	Data relating to a living individual who can be identified from that data or by other data which is in possession of or likely to come into the possession of the partner organisation. It includes any expression of opinion about an individual and any indication of the intentions of the data holder(s) in respect of the individual.
PROCESSING	Any operation performed on data. Main examples are collect, retain, use, disclosure and deletion. The use / reason for which information is stored or processed.
<i>PURPOSE</i>	
RECIPIENT	Anyone who receives personal information except statutory bodies for the purpose of specific inquiries Two levels of structure:
<i>RELEVANT FILING SYSTEM</i>	(i.) Filing system structured by some criteria (ii.) Each file structured so that particular information is readily accessible
SENSITIVE PERSONAL DATA	Personal data consisting of the following in relation to an individual: <ul style="list-style-type: none"> • their racial or ethnic origin, • Their political opinions • Their religious beliefs or other beliefs of a similar nature • Whether they are members of a trade union • Their physical or mental health or condition • Their sexual life • Their commission (or alleged commission) of an offence • Information relating to any legal proceedings with regard to an offence (or alleged offence)
<i>SUBJECT ACCESS</i>	The individual's right to obtain a copy of information held about himself or herself.

- i. Where the permission of the original provider of the information is required prior to secondary disclosure how will that permission be obtained and recorded?
- j. How long will the information be retained?
- k. What are the arrangements for secure storage and destruction of the information?
- l. What are the arrangements for subject access to the information?
- m. In what circumstances would it be reasonable for the data subject to be given access to their information without the specific consent of the original provider?
- n. Where the consent of the original provider is required before giving subject access how will it be obtained and recorded?
- o. What are the arrangements for rectifying errors in data

4. INFORMATION TO DATA SUBJECTS

- ⌚ What information are data subjects given about the purposes for which their information may be used, with whom it may be shared, how they can access it and rectify errors and how they might complain about the way their information has been used

5. BREACHES OF CONFIDENTIALITY

How are you going to deal with:

- ⌚ any breach of agreement by staff,
- ⌚ monitoring security incidents, and
- ⌚ complaints about data sharing which involve more than one agency and notification to the Head of the Information Management Group of Ealing Council

6. STAFF AWARENESS AND TRAINING

- ⌚ What are the arrangements for this?

7. GOVERNANCE

- I. Named individuals to lead on ISA
- II. Who will monitor compliance with the ISA

8. REVIEW OF INFORMATION SHARING AGREEMENT

- ⌚ How long will the ISA last
- ⌚ When will the ISA be reviewed

25 Ealing information sharing protocol **January 2007** Appendix C: information sharing agreement

9. CLOSURE/TERMINATION OF AGREEMENT

- ⌚ What will happen if there is a serious breach of confidentiality?
- ⌚ How will the Partners be able to terminate the agreement?

10. SIGNATORIES

This agreement is signed on behalf of:

Name of organisation:

Name of officer:

Title:

Date:

Name of organisation:

Name of officer:

Title:

Date:

Ealing