

London Borough of Brent

Overarching inter-agency  
Information Sharing  
Protocol

Published June 2005

# Introduction

Effective information sharing and information governance are a key aspect of the work of all public sector organisations. It is therefore important that partner agencies in Brent commit to mechanisms that help remove potential barriers to information sharing. Establishing an agreed overarching inter agency information sharing protocol is one such mechanism.

This Protocol is jointly approved by six partner agencies in the London borough of Brent.

The Protocol document is a high level written commitment outlining the framework and principles for sharing information about service users, agreed between party agencies in the London borough of Brent in order to support, protect and care for local individuals and communities.

The purpose of the Protocol is to further joined up working by encouraging all staff to lawfully share information based on the knowledge that an inter agency approved framework is in place.

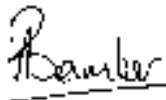
The Protocol is signed by those senior officers with authority to bind their agencies to such standards and enable the implementation of these standards in their agencies.

# Adoption of the Protocol

By adopting this Protocol, the parties agree and accept that the principles outlined in the document provide a secure overarching framework for the sharing of information between the respective organisations, in compliance with their statutory and professional responsibilities.

## Signatories

This overarching interagency Information Sharing Protocol is signed by the Chief Executives of each partner agency on behalf of their organisation.



**Andrew Bamber**

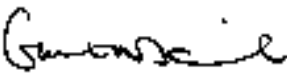
Borough Commander, Metropolitan Police Service



**Dr Peter Carter**

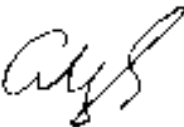
Chief Executive,  
Central & North West London Mental Health Trust

Central and North West London  
Mental Health NHS Trust



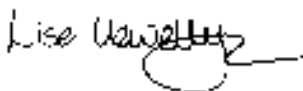
**Gareth Daniel**

Chief Executive, Brent Council



**Gerard Hollingworth**

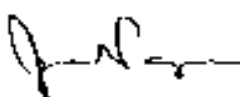
Borough Commander, London Fire Brigade



**Lise Llewlynn**

Chief Executive, Brent Teaching Primary Care Trust

**Brent NHS**  
Teaching Primary Care Trust  
Working with our partners for a healthier Brent



**John Pope**

Chief Executive,  
The North West London Hospitals NHS Trust

The North West London Hospitals  
NHS Trust



# Contents

Introduction	i
Adoption of the Protocol	1
<b>1 Background and Summary</b>	<b>3</b>
1.1 Why is sharing information so important?	
1.2 Benefits of the Information Sharing Protocol	
<b>2 The Information Sharing Protocol</b>	<b>4</b>
2.1 Parties to the Protocol	
2.2 Objectives	
2.3 Scope	
2.4 Key legislation and guidance	
2.5 Principles governing the sharing of information	
<b>3 Freedom of Information Act (FOIA) 2000</b>	<b>7</b>
3.1 Decision-making	
3.2 Code of Practice – transferring requests	
<b>4 Operational Procedures</b>	<b>8</b>
4.1 The common procedures	
4.2 Transfer of personal information	
4.3 Compromise of confidentiality	
<b>5 Implementation and dissemination</b>	<b>9</b>
5.1 Implementation	
5.2 Dissemination	
<b>6 Monitoring and reviewing arrangements</b>	<b>10</b>
6.1 Monitoring	
6.2 Reviewing	
<b>Appendix 1</b>	<b>11</b>
Detailed key legislation for information sharing	
<b>Appendix 2</b>	<b>15</b>
Checklist for service specific information sharing agreement (ISA)	

# 1 Background and Summary

## 1.1 Why is sharing information so important?

Information sharing and governance have increasingly been emerging as high priority in many government initiatives e.g. the Single Assessment Process (SAP) which allows health and social care agencies to work together to benefit users and carers. The Caldicott Report (1997) outlined principles regarding the flows of person identifiable information in the NHS. More recent developments have given a renewed emphasis to the importance of inter-agency information sharing, namely, the Bichard inquiry and the Children Act 2004.

There is an obligation for all local authorities to commit themselves and partner agencies to local mechanisms that help remove barriers to sharing information and further put in place structures to support information governance arrangements. Establishing an agreed overarching inter-agency protocol for sharing information is one step closer to good practice around improving information sharing arrangements.

Current practice on the ground in relation to information sharing varies considerably. Some staff may be reluctant to share information about service users because of uncertainties about current legislation and guidance. Other staff may be continuing to share information on the basis of informal arrangements.

Government requirement and good practice recommends that agencies draw up and implement inter-agency information sharing policies, setting the standards for and stating the legislative framework that will facilitate the transfer of information on a need to know basis for justifiable purposes.

## 1.2 Benefits of the Information Sharing Protocol

This overarching Protocol is a high level commitment, outlining the framework and standards between party organisations in the London Borough of Brent that are sharing information to protect, support and care for local individuals and communities. Without such formal arrangements, organisations can often find themselves falling short of common standards and confused over responsibilities.

The framework and standards outlined in this document are intended to be a tool – not a bureaucratic hurdle to be overcome. The purpose of the Protocol is to set out the overarching ground rules for sharing information that all partner agencies agree to. This will encourage staff to share information based on the knowledge that an inter-agency approved framework is in place.

### Note:

- The Protocol is signed by those senior officers with authority to bind their agencies to such standards and cause the implementation of these standards in their agencies.
- The Protocol should be used as a set of good practice standards that the parties need to meet in order to fulfil any duty of care which exists in relation to the sharing of personal information.
- This overarching Protocol needs to be supported by service specific information sharing agreements (ISAs), where necessary. The ISAs become the practical implementation of the overarching Protocol by stating specifically what, when, how, and between whom the information will be exchanged. A checklist for a standard ISA is incorporated in Appendix 2.

## 2 The Information Sharing Protocol

### 2.1 Parties to the Protocol

The following Brent organisations are parties to the Protocol:

- Brent Council
- Brent Fire Brigade
- Brent Police
- Brent Teaching Primary Care Trust (TPCT)
- Central & North West London Mental Health Trust
- North West London Hospitals NHS Trust

**Note:** Any national projects managed by these organisations will also be covered by this Protocol, and in some cases will need to be supported by specific ISAs for their specific exchange of information.

### 2.2 Objectives

- The Protocol records the parties' commitment and agreement to the framework and standards in relation to information sharing, laid out in the Protocol.
- It states and helps ensure compliance with the legislative framework that allows information to be shared effectively. For instance The 1998 Data Protection Act stipulates that organisations must satisfy themselves that the agencies they share information with have the necessary procedures in place to comply with the Act's requirements.
- It describes the principles which ensure that information is disclosed in line with statutory responsibilities.
- It outlines the common operational procedures that underpin the process for exchanging information.
- It describes how the Protocol will be implemented, monitored and reviewed.
- The Appendix contains comprehensive details that are relevant to all information sharing arrangements. This means that there is no need to keep "re-inventing the wheel" when drafting service specific Information Sharing Agreements (ISAs). As a consequence, individual ISAs can be relatively brief documents that focus on the specific types of information to be shared and any additional requirements that are felt to be necessary.

### 2.3 Scope

- The Protocol covers all ages of service users.
- The focus is primarily on the sharing of 'personal' and 'sensitive' information about people using associated services commissioned by the partner agencies listed in Section 2.1. ('Personal data' and 'sensitive data' are defined as in the Data Protection Act 1998 – see Appendix 1.)
- The document refers to 'private' and 'confidential' information in relation to the Human Rights Act 1998. (see Appendix 1)
- The aim is to provide strategic direction for information governance in a dynamic multi-agency environment.
- This is a tool to inform managers and frontline staff of the reasons why personal information about service users may need to be shared and how this sharing will be managed.

### 2.4 Key legislation and guidance

There are legal requirements surrounding information sharing that must be considered and complied with to ensure an individual's rights are respected. Organisations should put in place standards and procedures to ensure they do not breach these legal requirements.

The main pieces of legislation governing an individual's rights in respect of information sharing are:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- The Adoption Act 1976
- The Mental Health Act 1983
- The Service users Access to Records Act 1987 & Regulations 1989
- The Copyright Designs and Patents Act 1988
- The Children Act 1989
- The Children Act 2004
- The Computer Misuse Act 1990
- The NHS & Community Care Act 1990
- The Access to Health Records Act 1990
- The Carers (Recognition & Service) Act 1995

- The Crime & Disorder Act 1998
- The Health Act 1999 (section 31)
- The Regulation of Investigatory Powers Act 2000
- The Health and Social Care Act 2001 (Section 60)
- The Learning and Skills Act (2001)
- The NHS confidentiality code of practice

**Note:** Appendix 1 provides further detail on specific law relevant to sharing information.

### 2.5 Principles governing the sharing of information

A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing information appropriately. The key principles governing the sharing of information are detailed in the Data Protection Act 1998 and the Caldicott Report 1997. The Human Rights Act and the common law “duty of confidentiality” are also relevant in this context.

However, it is recognised that multi-agency initiatives require a commitment to sharing personal information about service users in order to provide a quality and timely service. The sharing of information by partner organisations under the Protocol will be based primarily on the following principles. It is envisaged that each agency will provide training to their staff on outlined principles.

#### 2.5.1 Statutory duties

Partner organisations ensure that they share information in accordance with their statutory duties including the requirements of the Data Protection Act 1998 and the Human Rights Act 1998.

#### 2.5.2 Caldicott requirements

All organisations recognise and understand the requirements that Caldicott imposes on health and social services departments. They will ensure that requests for information from these organisations are dealt with in a manner compatible with these requirements.

#### 2.5.3 Duty of confidentiality

All organisations that are party to this Protocol accept this duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.

#### 2.5.4 Consent

Wherever possible and appropriate, organisations should seek consent from the service user to share personal information. The service user or data subject will be made fully aware of the information it is proposed to share and the purposes for which it will be used.

#### 2.5.5 Sharing without consent

Organisations will put procedures in place to ensure that decisions to share personal information without consent have been fully considered and comply with the requirements of the relevant legislation. Such decisions will be appropriately recorded for audit purposes. All staff will be made aware of the roles and responsibilities of the Data Protection Officer and/or the Caldicott Guardian should they need advice regarding sharing without consent.

#### 2.5.6 “Need to know”

Where it is agreed necessary for information to be shared, this will be done on a “need-to-know” basis only, i.e. the minimum information, consistent with the purpose for sharing, will be given.

### 2.5.7 Specific purpose

Information received from partners will only be used for the purpose(s) for which it was disclosed.

### 2.5.8 Use of anonymised information where possible

Personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes, information about individual cases will be anonymised.

### 2.5.9 Access to information

People will be fully informed about the information that is recorded about them (Fair Processing Notices / Privacy Statements). They will be able to gain access to information held about them and to correct any factual errors that may have been made. If an organisation has statutory grounds for restricting a person's access to information about them, they will be told that such information is held and the grounds on which it is restricted. Where opinion about a service user is recorded and they feel the opinion is based on incorrect factual information, they will be given the opportunity to correct the factual error and record their disagreement with the recorded opinion.

### 2.5.10 Complaints procedures

Partners are committed to having procedures in place to address complaints relating to the disclosure of information. Service users will be provided with information about these procedures.

### 2.5.11 Staff awareness

Partner organisations will ensure that all relevant staff are aware of and comply with their responsibilities in relation to the:

- Information Sharing Protocol
- Confidentiality of information about service users
- Commitment to share information in accordance with guidance and legislation

## 3 Freedom of Information Act (FOIA) 2000, Dealing with inter-agency requests

### 3.1 Decision-making

All decision-making processes about the disclosure/non-disclosure of information in inter-authority requests will only be resolved by real-time case conferencing or email exchange. In all cases such decisions will be fully recorded and communicated to the applicant.

Agreement should be reached on the disclosure or non-disclosure of information wherever possible, and that the fullest consideration should be given to an authority's claim to the application of an exemption.

There will be rare cases where the dispute between two agencies cannot be resolved about the disclosure or non-disclosure of information. The receiving agency is guided to consider the option of non-disclosure of the information. This will enable the applicant, if not satisfied with the outcome, to proceed to a complaint stage where the decision-making process can be reviewed by the receiving agencies' internal complaint process. However, it is recognised that ultimately it is for the public body receiving the request to determine whether a disclosure should be made. This will enable the applicant, if not satisfied with the outcome, to proceed to a complaint stage where the decision-making process can be reviewed by the receiving authority's internal complaint process.

The legal obligation is clear – an agency receiving a request for information that it holds has a duty to disclose that information unless an exemption applies – this ensures that inter-agency requests are dealt with in a manner that will provide the best service to the applicant and ensure that decisions on the disclosure or non-disclosure of information are dealt with in a co-ordinated approach.

### 3.2 Code of Practice – transferring requests

The Code under s.45 FOIA outlines further responsibilities on a public body to transfer requests for information that it does not hold, where it is believed to be held by another organisation. The public body will consider whether to:

- consult the other organisation with a view to establishing whether information is held
- transfer the request, either in full or the part of the request that relates to information held elsewhere, with the consent of both the applicant and the other agency

The receiving agency must still advise the applicant that it does not hold the information (or part of it), consider the appropriateness of advising the applicant that the information is held elsewhere and seek the applicant's consent to transfer the request. Information held by the receiving agency that can be disclosed must be so disclosed whilst the remainder of the request is transferred. The FOIA officer within each organisation is responsible for this process.

## 4 Operational procedures

A key aspect of the Protocol is the adoption by partners of operational procedures for the sharing of information. This is intended to give confidence to organisations and service users that, when information is being shared, partner agencies will be operating to a common standard that complies with relevant legislation and guidance.

(It is acknowledged that partner organisations may already have procedures in place that meet these standards and will want to use these)

### 4.1 The common procedures are briefly outlined here

- Organisations should put in place arrangements for establishing where necessary, service specific information sharing agreements (ISAs). A checklist for a standard information sharing agreement is included in Appendix 2.
- Organisations should identify designated officers who will manage this overarching inter-agency Information Sharing Protocol and be prepared to fully train staff.
- Training should be provided to all practitioners, information gathering staff and input staff such as admin and information officers on good practice when sharing information e.g. seeking consent, and recognising and implementing good record management practice.
- Contact details for staff with specific responsibilities should be circulated.
- Information access and security procedures should be in place e.g. when transferring information by fax, e-mail, verbally, post.

### 4.2 Transfer of personal information

- All agencies will put in place policies and procedures that govern the secure transfer of person-identifiable information both internally and externally. Such policies and procedures must cover:
  - Internal and external postal arrangements
  - Verbal, face-to-face, telephone
  - Facsimiles
  - Electronic mail (secure network or encryption)

### 4.3 Compromise of confidentiality

- All agencies will have in place appropriate measures to investigate and deal with inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.
- In the event of personal information that has been shared under the Protocol having or may have been compromised, whether accidental or intentional, the agency making the discovery will without delay:
  - Inform the information provider of the details.
  - Take steps to investigate the cause.
  - If appropriate, take disciplinary action against the person(s) responsible.
  - Take appropriate steps to avoid a repetition.
- On being notified that an individual's personal information has or may have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary:
  - Notify the individual concerned.
  - Advise the individual of their rights.
  - Provide the individual with appropriate support.

# 5 Implementation and dissemination

## 5.1 Implementation

The partner organisations agree to:

- Ensure that all staff within their organisation adhere to the principles set out in the Protocol.
- Put in place mechanisms to meet the standards and procedures outlined in the Protocol.
- Provide training and awareness of key principles of information sharing as outlined in section 2.5 of this document.

## 5.2 Dissemination

Partner agencies will take individual responsibility in the dissemination of the Information Sharing Protocol within their agencies. This could be done in many ways:

- Staff inductions: An overview of the Protocol should be available for inclusion in staff induction programmes.
- Regular staff communication: As and when the Protocol is amended (following review), programmes should be arranged to inform staff of agreed changes.
- Training sessions for relevant staff on understanding of and implementation of the Information Sharing Protocol.
- Notice for the public: Fair Processing Notice and Privacy Statement to the public.
- Inform those staff involved directly with aspects of information sharing and governance e.g. Data Protection Officer, Information Governance Leads and the Caldicott Guardian etc.
- Regular reports to strategic boards.

In addition:

- All partners should make copies available to service users, carers and members of the public.
- The Protocol should be available on the websites of the respective agencies.

## 6 Monitoring and reviewing arrangements

### 6.1 Monitoring

Partner agencies will take individual responsibility in monitoring and reviewing the implementation of the Protocol in their agency. This could be done in many ways:

- Monitoring how many briefing sessions have taken place explaining the implications of the Information Sharing Protocol.
- Monitoring the number of queries regarding information sharing after the formal adoption of the Protocol, in comparison to previous times.
- Ensuring current service specific information sharing agreements are fully compliant and consistent with the overarching Inter-agency Protocol.
- Addressing the training needs in relation to information sharing.

### 6.2 Reviewing

The Protocol will initially be reviewed six months after sign off and then on an annual basis.

# Appendix 1

## The law and Principles relevant to information sharing

This appendix is provided as a general guide. If you have a need for more detailed guidance this should be sought from your organisation's designated officers such as the Data Protection Officer, Information governance leads, Caldicott guardian or legal advisors.

In alphabetical order

### Caldicott principles

The Caldicott Committee (which reported in 1997) 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.

**1. Define Purposes** Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

**2. Use anonymised information if possible** Patient-identifiable information items should not be included unless it is essential for the specified purpose. The need for patients to be identified should be considered at each stage of satisfying the purpose.

**3. Use the minimum information necessary** The minimum amount of identifiable information should be transferred or made accessible that is necessary for a given function to be carried out.

**4. Access to personal information on a need to know basis:** Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

**5. Staff must be aware of their responsibilities** Action should be taken to ensure that those handling patient-identifiable information - both clinical and

non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**6. Use only when lawful** Every use of patient-identifiable information must be lawful.

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.

### Common Law Duty of Confidentiality

The Common Law Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest i.e. to protect others from harm.

### Crime and Disorder Act 1998

The Act is concerned with measures to reduce crime and disorder and includes the introduction of local crime partnerships to formulate and implement strategies for reducing crime and disorder in each local authority area.

Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (where they would not otherwise have the power). Guidance from the Information Commissioner suggests that this power can be used to support anti-crime initiatives by these agencies generally and not just for the purposes of obtaining one or more of the various orders specified in the Act.

Under Section 17 each police authority and local authority is required to exercise its functions with due regard to the need to do all it reasonably can to prevent crime and disorder in its area.

## Criminal Procedures and Investigations Act 1996

This Act requires the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service, who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case.

In cases where the information is deemed to be of a sensitive nature then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

## Data Protection Act 1998

A few definitions may help in understanding the language of the Act:

- Data processing: applies to anything at all done to personal data, including collection, use, disclosure (sharing), destruction and merely holding data.
- Data controller: organisations processing personal data.
- Data subject: the individual service user about whom personal data is held and used.

The key law that governs sharing of personal information is the Data Protection Act 1998 (the D.P Act).

The Data Protection Act provides eight guiding principles. They apply to information about a living person, where that person could be identified from that information. As such, they do not apply to anonymised information, but care needs to be taken with information covering small areas / groups, where individuals could still be identified.

The eight guiding principles of the data protection act:

**1. Fair and lawful** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met. Also the processing must adhere to the fair processing code

**2. Use for specified purposes** Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

**3. Adequate, relevant and not excessive** Personal data shall be adequate, relevant and not excessive in relation to the purpose

**4. Accurate and up to date** Personal data shall be accurate and, where necessary, kept up to date.

**5. Don't keep longer than necessary** Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

**6. Rights given under the act** Personal data shall be processed in accordance with the rights of the data subject under this act".

**7. Security** Appropriate and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

**8. Disclosure outside Europe** Personal data shall not be transferred to a country or territory outside the European Economic area, unless that country or territory ensures an adequate level of protection

## Schedule 2 and Schedule 3 conditions

- Condition for processing personal data is that 1 condition in Schedule 2 should be met.
- Condition for processing sensitive personal data is 1 condition in Schedule 2 and a condition in Schedule 3 should also be met.

## Schedule 2: Personal data

The data subject has given consent, or the processing is necessary for:

- A contract
- Legal obligation
- Protection of the vital interests of the data subject
- Public function
- In the public interest
- A statutory obligation
- Legitimate interests of the Data Controller

## Schedule 3: Sensitive personal data

The data subject has given explicit consent, or the processing is necessary for:

- Employment related purposes
- The purpose of, or in connection with legal proceedings.
- Protection of vital interests of the individual (where consent cannot be obtained).
- Made public by the data subject
- Substantial public interest
- Prevention or detection of an unlawful act
- Legitimate interests of a nonprofit making organisation.
- Medical purposes

## Freedom of Information Act 2000

The Freedom of Information Act provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector.

The legislation will apply to a wide range of public authorities, including Parliament, Government Departments and local authorities, health trusts, doctors' surgeries, publicly funded museums and thousands of other organisations.

The main features of the Act are:

- A general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions;
- In most cases where information is exempted from disclosure there is a duty on public authorities to state where they believe the public interest in disclosure outweighs the public interest in maintaining the exemption in question;
- A new office of Information Commissioner and a new Information Tribunal, with wide powers to enforce the rights created;
- A duty imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the Commissioner, will specify the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee.

## Health and Social Care Act 2001 (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. (Note that as of February 2002 the regulations which are needed to give effect to Section 60 have not yet been passed.)

## Human Rights Act 1998

Article 8.1 of the Act provides that "everyone has the right to respect for his private and family life, his home and his correspondence." European case law shows that storing or using "private" information, or disclosing this information for a purpose other than the purpose for which it was originally obtained will all constitute an interference with these rights. This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights. Article 8.2 defines the grounds as follows:

- In the interests of national security, public safety, or the economic well-being of the country
- For the prevention of disorder or crime
- For the protection of health or morals
- For the protection of the rights and freedoms of others.

In addition to identifying one of these grounds, a public body would also have to show:

**"proportionality"** i.e. that it had tried to strike a fair balance between the individual's rights and the permitted ground for interference it was seeking to rely on. In the event of a claim that an organisation has acted in a way which is incompatible with the Act, the key factors that will be considered will include:

- Whether the organisation can show that it has taken the rights under the Act into account in reaching its decision;
- That it considered whether any breach may result, directly or indirectly, from its action;
- If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
- Whether one of the permitted grounds for interference could be relied upon;
- Whether there was proportionality.

The Act also requires public bodies to read and give effect to other legislation in a way which is compatible with these rights and makes it unlawful to act incompatibly with them. As a result these rights still need to be considered, even where there are special statutory powers to share information.

### Regulation of Investigatory Powers Act 2000

This legislation ensures that investigatory powers are used in accordance with human rights.

### Statutory restrictions on passing on information

There are statutory restrictions on passing on certain types of information.

- 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 2

## Checklist for Information Sharing Agreements (ISAs)

### What is an Information Sharing Agreement?

An information sharing agreement is a specific agreement for a particular service area. This is drawn up by two or more organisations that need to share personal information about service users. As the Overarching Inter-agency Information Sharing Protocol provides the common framework and principles for sharing information, the Information Sharing Agreement (ISA) need only refer to these and provide just specific information about the particular arrangements.

The guidelines below provide useful headings which should be incorporated into all specific Information Sharing Agreements. ISAs do not need to be lengthy documents.

### Section 1: Background

- Scope: multi-agency involvement across borough boundaries.
- Reference to the Overarching Information Sharing Protocol.
- Objectives of the services party to this agreement.
- Why is an agreement required? E.g. nature of the work etc.
- Purpose for which information needs to be shared.

### Section 2: Procedures

- What type of information will be held name, address, DOB, family situation etc.
- Procedures relating to security and confidentiality - Recording, verification and security of information e.g. checking for accuracy when recording information.
- Procedures on seeking consent to share information e.g. are staff trained, forms, what if consent is not given? Issues around Gillick Competency.
- Duration of information sharing e.g. destruction of information after the project is over.
- Use of depersonalised information for evaluation.
- Procedures around CRB (criminal records bureau) checks.

- Ensuring that the agency is registered with the Information Commissioners Register.
- Information governance and security policies in place e.g. taking laptops / information home.
- Procedures to manage the agreement e.g. disseminating & training; monitoring & reviewing.
- Breaches of agreement.
- Indemnity
- Staff roles that should have access to this information
- Methods of transfer (e.g. fax, e-mail, phone)

### Section 3: Adoption

- Parties to the agreement
- Structures and responsibilities of staff
- Which specific legislation / Principles apply to this agreement?
- Privacy statements to service users.
- Named contact for further information.
- Review Date (6 monthly, annually – depending on the length and nature of sharing).
- Formal sign off section.







[www.brent.gov.uk](http://www.brent.gov.uk)

Published by  
London Borough of Brent information  
Sharing & Assessmnets (ISA)  
TEL 020 8937 3074  
Designed by Brent Design Unit  
06.05 BDU 4824