

INTER-AGENCY INFORMATION SHARING PROTOCOL

DOCUMENT CONTROL

Author	SWYMHT in conjunction with the Information Sharing Protocol Review Group
Contributors	All signatory agencies
Version	Final version 5
Date of Production	February 2009
Date due for revision	February 2012
Post responsible for revision	Information Sharing Protocol Review Group
Primary Circulation list	All Signatory Organisations
Number of document	N/A
Restrictions	None

Contents	Page
1. Purpose of the Protocol.....	4
2. Background.....	6
2.1 Legislative Context.....	6
2.2 Local Context.....	7
3. Principles, Guiding the Sharing of Information.....	7
4. Consent.....	8
5. Supporting Policies and Procedures.....	10
5.1 Supporting Policies.....	10
5.2 Access and Security Procedures.....	11
5.3 Induction and Continuing Education.....	11
5.4 Data Quality.....	11
6. Approval, Implementation and Review.....	12
6.1 Agreeing the Protocol.....	12
6.2 Implementation.....	12
6.3 Monitoring and Review Processes.....	13
7. Conclusion.....	13

Appendices

Appendix I - Summary of Key Legislation and Guidance

Appendix II - Standard requirements for an information protocol

Appendix III - Memorandum of Agreement and signature sheet

Appendix IV - Current signatories

Glossary of Terms:

Agencies

Used in the context of this document to relate to the organisations specified within appendix iv which details the organisations that are signatories to this protocol.

Anonymised Information

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.

Disclosure

This is the divulging or provision of access to data.

Explicit Consent

This means articulated agreement and relates to a clear and voluntary indication of preference of choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

Implied Consent

This means agreement that has been signalled by the behaviour of an individual with whom a discussion has been held about the issues and therefore understands the implications of the disclosure of information.

Information Sharing Protocol

The protocol is the high level document setting out the general reasons and principles for sharing data. The protocol will show that all signatory agencies are committed to maintaining agreed standards on handling information and will publish a list of senior signatories. It should be underpinned by information sharing agreements between the organisations who are actually sharing the information.

Information Sharing Agreement

The agreement is a more detailed document the intention of which is to spell out how the organisations involved will operate the approach to information sharing. Agreements will be produced where organisations specifically identify a purpose to share information across organisational boundaries. The agreement should state whether partners are obliged to, or are merely enabled to, share data.

INTER-AGENCY INFORMATION SHARING PROTOCOL

1. Purpose of the Protocol

Local agencies are increasingly working together. To work together effectively agencies need to be able to share information about the services they provide and the people they provide these services to.

This protocol covers the sharing of person-identifiable confidential information, with the individual's express consent, unless a legal or statutory requirement applies for the following purposes:

- Provision of appropriate care services
- Improving the health of the population
- Protecting people and communities
- Supporting people in need
- Supporting legal and statutory requirements
- Managing and planning services (where information has been suitably anonymised)
- Commissioning and contracting services (where information has been suitably anonymised)
- Developing inter-agency strategies
- Performance management and audit
- Research (subject to the Research Governance Framework)
- Investigating complaints or serious incidents
- Reducing risk to individuals, service providers and the public as a whole
- Clinical Audit
- Monitoring and protecting public health
- Common Assessment Framework
- Staff management and protection
- To fulfil responsibilities in law such as; Data Protection Act (1998), Human Rights Act (1998), Common Law, Crime and Disorder Act (1998), Mental Health Act (1983), Fertilisation and Embryology Act (1990), NHS (Venereal Diseases) 1974 Regulations and the Children Act (2004).

This is not intended to be an exhaustive list. If, as a result of policy changes or other developments, additional information sharing requirements arise these will be added to the protocol.

This protocol does not give carte blanche licence for the wholesale sharing of information. Information sharing must take place within the constraints of the law and relevant guidance and service specific requirements.

This protocol will be underpinned by service specific operational agreements that are designed to meet the specific information sharing needs of that service.

The purpose of this protocol is:

- To provide the basis for an agreement between the local agencies, and other associated organisations, to facilitate and govern the effective and efficient sharing of information. Such information sharing is necessary to ensure that individuals, and the population as a whole, can and do receive the care, protection and support they may require.
- To identify the purposes for which information may be shared. This document is supported by local operational policies and procedures within each agency that underpin the secure and confidential sharing of such information
- To promote and establish a consistent approach between the agencies to the development and implementation of information sharing agreements and procedures.

A further purpose of the protocol is to establish arrangements for the sharing of large datasets between organisations. Following the Government's publication in 2006 of the 'Information Sharing Vision Statement', and as part of the Service Transformation Plans, a cross-government programme has been established with the aim of overcoming barriers to information sharing within the public sector.

The key areas where information sharing could be beneficial include:

1. sharing for the purposes of law enforcement and public protection
2. sharing to provide or improve services in the public, private and voluntary sectors
3. sharing to facilitate statistical analysis and research.

Consent to share should be sought through agreements at the point of data collections. Data-sharing practices and schemes should be published and maintained as required under the Freedom of Information Act. Organisations should publish and regularly update a list of those organisations with which they share and exchange personal information.

Examples of where large datasets may need to be shared includes the management of Contact Point, where responsibility for the data supplied to the national system rests with the Local Authority, but data is supplied from a wide number of agencies, including Health and the Voluntary Sector. A Data Sharing agreement would cover the purposes, accountability, restrictions imposed and secure transfer arrangements where data has been shared for this purpose. Each occasion of data sharing of this type will need its own Data Sharing Agreement.

Requests to share datasets must relate to one or more of the three key areas identified above and should contain only demographic details, such as a geographical reference, age, gender and possible ethnicity information.

As such this document:

- **Informs** about the reasons why information may need to be shared and how this sharing will be managed and controlled by the agencies concerned.
- **Identifies the local agencies** that are party to this protocol.
- **Sets out the principles** that underpin the exchange of information between agencies.
- **Defines the purposes** for which agencies have agreed to share information.
- **Describes the policies and procedures** that support the sharing of information between agencies and will ensure that such sharing is in line with legal, statutory and common law responsibilities.
- **Promotes a standard approach** to the development of information sharing agreements and procedures.
- **Sets out the process** for the implementation, monitoring and review of the protocol.

2. **BACKGROUND**

2.1 **Legislative context and national guidance documentation**

All agencies are subject to a variety of legal, statutory and other guidance in relation to the sharing of person- identifiable or anonymised information.

For all agencies the key legislation and guidance affecting the sharing and disclosure of information includes (but is not necessarily an exhaustive list): -

Legislation:

- Access to Health Records 1990
- Data Protection Act 1998
- Crime and Disorder 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- The Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education Act 2002
- Mental Capacity Act 2005
- Local Government Act 2000
- Homelessness Act 2002

Appendix I provides summary details of the above-mentioned, and related, legislation and guidance.

2.2 Local Context

All agencies face similar requirements with regards to the development of information sharing agreements with their local partners. While the requirements remain similar the number of partners with which an agency must have such agreements differs. This number is dependent on the geographical area covered by an agency and the nature of its work.

This protocol is a recognition that consistent information sharing agreements now need to exist across the local government boundaries .

The intention of this protocol is to support and build on existing agreements in order to provide a common process for the development and implementation of future information sharing agreements across the patch.

The protocol is aimed at the information sharing agreements required between agencies and provides a framework within which agencies can share information.

3. Principles guiding the sharing of information

The following key principles guide the sharing of information between the agencies:

- 3.1** Agencies endorse, support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymised information where such information sharing is essential for the provision of effective and efficient services to the local population.
- 3.2** Agencies are fully committed to ensuring that if they share information it is in accordance with their legal, statutory and common law duties, and, that it meets the requirements of any additional guidance.
- 3.3** All agencies have in place policies and procedures to meet the national requirements for Data Protection, Information Security and Confidentiality. The existence of, and adherence to, such policies provides all agencies with confidence that information shared will be transferred, received, used, held and disposed of appropriately.
- 3.4** Agencies acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of information from other agencies employees and contracted volunteers will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately. This responsibility also extends to third party disclosures, any proposed subsequent re-use of information which is sourced from another agency should be approved by the source organisation.
- 3.5** An individual's 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 should be anonymised.

- 3.6 Where it is agreed that the sharing of information is necessary, only that which is needed and relevant will be shared and that would only be on a “need to know” basis.
- 3.7 When disclosing information about an individual, agencies will clearly state whether the information being supplied is fact, opinion, or a combination of the two.
- 3.8 There will be occasions when it is legal and necessary for agencies to request that information supplied by them be kept confidential from the person concerned. Decisions of this kind will only be taken on statutory grounds and must be linked to a detrimental effect on the physical or mental wellbeing of that individual or other parties involved with that individual. The outcome of such requests and the reasons for taking such decision will be recorded.
- 3.9 Careful consideration will be given to the disclosure of information concerning a deceased person, and if necessary, further advice should be sought before such information is released.
- 3.10 Agencies will ensure that all relevant staff are aware of, and comply with, their responsibilities in regard both to the confidentiality of information about people who are in contact with their agency and to the commitment of the agencies to share information.
- 3.11 All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally could be subject to disciplinary action.
- 3.12 Organisations/agencies are responsible for putting into place effective procedures to address complaints relating to the disclosure of information, and information about these procedures should be made available to service users.

4. Consent

- 4.1 Information is provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case, or where a person receiving the information knows, or ought to know, that the information is being given in confidence. It is generally accepted that most (if not all) information provided by patient/clients is confidential in nature. All agencies, which are party to this protocol accept the duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds or an overriding justification for doing so. In requesting release and disclosure of information from members of partner organisations, staff in all organisations will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately, this includes third party disclosures.
- 4.2 Agencies are fully committed to ensuring that they share information in accordance with their statutory duties. They are required to put in place procedures that will ensure that the principles of the Data Protection Act and

requirements of other relevant legislation are adhered to and underpin the sharing of information between their organisations.

- 4.3** As is required by the fair processing requirements of the Data Protection Act 1998, individuals in contact with agencies will be fully informed about information that is to be obtained, held or disclosed about them. The individual has the right to request that processing of their information cease if there is undue damage or distress caused to them.
- 4.4** As a **minimum**, individuals will be informed that information may be shared and the circumstances in which this could happen unless this poses a risk of harm or danger. Fair processing notices should always be in place. Consent can often be inferred from the circumstances in which information was given. However, it is always important that the person giving consent understands who will see their information and the purpose to which it will be put. If there is any doubt as to whether a disclosure is supported by a legal, statutory requirement or an immediate serious risk explicit consent should be sought. Where an agency has consent forms the service user should be requested to sign one. Consent can be given verbally and recorded on the casenotes.
- 4.5** The individuals right to confidentiality are not absolute and may be overridden if evidence that disclosure for specific purposes is necessary in exceptional circumstances. Such as;
- Where it is required by statute
 - Where not to share the information poses a public health risk
 - Where there is a risk of harm to any person
 - Where sharing is required to prevent serious crime.

Where the individual chooses to exercise their right not to provide express consent for information sharing, they must be advised of any constraints that this will put upon the service that can be provided, however the individuals wishes must be respected unless there is a statutory requirement or a significant risk of harm to an individual to override those wishes as indicated above.

- 4.6** Where the individual is unable to provide express consent due to incapacity, the professional concerned must take decisions about the use of information. This must take into consideration the individual's best interests and any previously expressed wishes, or the wishes of anyone who is authorised to act on behalf of the individual. Information must only be disclosed that is in the individuals best interest, and only as much information as is needed to support their care.
- 4.7** Where the individual to whom the information relates is a child, e.g over the age of 12, and it is determined that the individual has the competency to make decisions regarding the sharing of information they have provided in confidence, their wishes must be respected. In other cases where the individual does not have the capacity to consent, express consent must be sought from the individual with parental responsibility (parent or guardian). Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults.

4.8 Safeguarding Children

- Safeguarding children is everyone's responsibility
- Mistreatment of any child is not acceptable
- Doing nothing is not an option
- Your actions can make a difference,

The over-riding principle that the welfare of the child is paramount must be central to any consideration about whether to share information. It is assumed that in all instances where there are concerns about a child's safety it is better to share the information than not. A failure to pass on information that might prevent a tragedy could expose professionals to criticism in the same way as an unjustified disclosure. In general the law will not prevent reciprocal sharing of information between practitioners if:

- Those likely to be affected have given consent; or
- The public interest in safeguarding the child's welfare overrides the need to keep information confidential; or
- Disclosure is required under a court order or other legal obligation

Safeguarding Adults

- Safeguarding adults is everyone's responsibility
- Mistreatment of any adult is not acceptable
- Doing nothing is not an option
- Your actions can make a difference

Vulnerable adults are part of our community and have specific needs that require us to work in a partnership with other agencies that also have responsibilities for their welfare. We share the responsibility to develop, implement and enforce policies and procedures in relation to 'Safeguarding Adults' issues. We are committed to providing training and development for all staff to support them in their safeguarding responsibilities.

- 4.9 Where professionals request that information supplied by them be kept confidential from the people who use services the outcome of this request and the reasons for taking the decision will be recorded. Decisions of this kind will only be taken on statutory grounds.

5. **SUPPORTING POLICIES, PROCEDURES AND GUIDANCE**

5.1 Supporting policies

For members of the public and staff from different agencies to have confidence that information sharing takes place legally, securely and within relevant guidance all agencies have in place policies which meet the requirements for:

- Data Protection
- Confidentiality
- Information Security

These policies must cover manual, verbal and computer-based information.

Processes must be in place within agencies to regularly monitor and improve the effectiveness of these policies.

5.2 Access and Security Procedures

All agencies will look to implementing technological solutions to support the safe transfer of data. Risk assessments will be carried out before the transfer of data is carried out and all reasonable steps to mitigate any risks identified will be taken. Supporting documentation relating to the secure transfer, receipt, access to, storage and disposal of shared information should be made available to staff.

Each organisation will keep a log of all requests for information sharing received.

Each organisation will instigate a system of reporting back to the originator of information where actions have been taken on the basis of the information shared.

Agencies should put into place policies, procedures or guidelines covering:

- Communication by fax
- Communication by phone
- Electronic communication
- Verbal communication
- Written communication
- Use of personal information for purposes other than that agreed
- Access arrangements to shared records and databases
- Secure storage and disposal of confidential information

These policies, procedures or guidelines should be subject to regular monitoring.

5.3 Induction and continuing education

To support the implementation of the above-mentioned policies and procedures appropriate staff induction and training programmes must be made available within the agencies.

5.4 Data Quality

Good data quality is an essential requirement to all data users and underpins the timely and effective delivery of services to those in need. Several characteristics of good data quality have been identified and in summary they are:

Accuracy – Data should be sufficiently accurate to present a fair picture of circumstances and enable informed decision-making at all appropriate levels. Definitions for data should be specific and unambiguous.

Validity – Data should represent clearly and appropriately the intended result and should be used in accordance with the correct application of any rules or definitions.

Reliability – Data should reflect stable and consistent data collection processes that need to be fit for purpose and incorporate controls and verification procedures.

Timeliness – Data input should occur on a regular ongoing basis rather than being stored to be input later. Verification procedures should be as close to the point of input as possible.

Relevance – Information collected should comprise the specific items of interest only. Sometimes definitions need to be modified to reflect changing circumstances in services and practices, to ensure that only relevant data of value to users is collected, analysed and used.

Completeness – All the relevant data must be recorded. Missing or invalid data can lead to incorrect judgement and poor decision-making.

6. Approval, implementation and review

6.1 Agreeing the protocol

This Protocol proposes a consistent approach to the development of information sharing agreements.

Appendix III provides outline of the formal agreement format.

6.2 Implementation

Following approval of the protocol agencies will need to take action, either individually or jointly, on the following issues:

Agencies	Actions
All agencies	<ul style="list-style-type: none"> • Promoting ownership of responsibilities associated with the protocol • Ensuring dissemination and appropriate implementation • Reviewing existing support policies, procedures and guidance. • Agreeing training programmes • Monitoring implementation/compliance • Establishing review processes • Joint work to develop standard service specific agreements • Ensuring amendments to existing agreements • Agreeing audit processes • Maintaining local registers of agreements.
Chief Officers/Boards of each organisation or department/Caldicott	<ul style="list-style-type: none"> • Annual review

6.3 Monitoring and review processes

Where not already in place processes will be set up in each agency to adopt a risk management approach to breaches/problems in relation to the implementation of this agreement. Formal review of the protocol should be held at three yearly intervals unless legislative changes require immediate action.

Prior to the review date, agencies should submit feedback on the use of the protocol and propose options for addressing problems or amending procedures.

It is proposed that reviews would, in the first instance, be co-ordinated through the Information Sharing Protocol Review Group.

7. Conclusion

All agencies are in the position of having to balance the conflicting demands of the need and requirement to share information with other agencies with the responsibility to maintain highest level of confidentiality.

This protocol acknowledges these competing demands and provides a means whereby members of the public, staff and the agencies can be confident that where information is shared it is done so appropriately and securely.

APPENDIX I

SUMMARY OF KEY LEGISLATION AND GUIDANCE

(detailed guidance should be available in all agencies for staff)

Access to Health Records Act 1990

This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased

Data Protection Act 1998

The key legislation governing the protection and use of identifiable patient/client information (Personal Data) is the Data Protection Act 1998. The Act does not apply to information relating to the deceased.

This Act gives seven rights to individuals in respect of their own personal data held by others. They are:

- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Rights in relation to automated decision making
- Right to take action for compensation if the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

In addition, the Act stipulates that anyone processing personal data comply with eight principles of good practice. These principles are legally enforceable.

Principle 1 – Personal data shall be processed fairly and lawfully

Principle 2 – Personal data shall be obtained only for one or more specified lawful purposes

Principle 3 – Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

Principle 4 – Personal data shall be accurate and, where necessary, kept up to date.

Principle 5 – Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that or those purposes.

Principle 6 – Personal data shall be processed in accordance with the rights of data subjects under this Act, including the right to access their own record.

Principle 7 – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss.

Principle 8 – Data shall not be transferred outside of the European Economic Area

Detailed information for staff about the requirements of the Act in relation to information sharing are available in each agency.

Crime and Disorder Act 1998

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local 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 (or persons acting on their behalf) where they do not otherwise have the power but only where it is necessary and expedient for the purposes of the Act. However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement on them to exchange information and responsibility for the disclosure remains with the agency that holds the data. It should be noted, however, that this does not exempt the provider from the requirements of the 2nd Data Protection principle.

The Criminal Procedures and Investigations Act 1996 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.

Human Rights Act 1998

Article 8.1 of the Human Rights Act 1998 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. 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 and Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right as it is in accordance with the law and is necessary in a democratic society 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 or for the protection of the rights and freedom of others”.

In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show in relation to its decision to take a particular course of action:

-

- That it has taken these rights into account
- That it considered whether any breach may result, directly or indirectly, from the action, or lack of 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 that 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 when there are special statutory powers to share information.

Common law duty of Confidentiality

All staff working in both the public and private sector are aware that they are subject to a common law Duty of Confidentiality and must abide by this. The duty of confidence only applies to identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e., it is not possible for anyone to link the information to a specified individual.

The 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 has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g., to protect others from harm). Whilst it is not entirely clear under law whether or not a common law Duty of Confidence extends to the deceased, the Department of Health and professional bodies responsible for setting ethical standards for health professionals accept that this is the case.

Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained (deceased individuals may have provided their consent prior to death). Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness) other conditions in schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the vital interest of the individual).

Whilst under current law, no-one can provide consent on behalf of an adult in order to satisfy the common law requirement, it is generally accepted that decisions about treatment and the disclosure of information should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

All agencies are subject to their own codes or standards relating to confidentiality.

Caldicott Report 1997

The Caldicott Committee (which reported in 1997) recommended a series of principles that should be applied when considering whether confidential information should be shared. The principles have been developed with the aim of establishing the highest practical standards for handling confidential information. They apply equally to all routine and ad hoc flows of patient information whether clinical or non-clinical, in manual or electronic format. The principles are:

- Justify the purpose(s) for using confidential information

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.

- Only transfer/use patient-identifiable information when absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose.

- Use the minimum identifiable information that is required

Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

- Access should be on a strict need to know basis

Only those individuals who need access to patient-identifiable information should have access to it. 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 flow is used for several purposes.

- Everyone with access to identifiable information must understand his or her 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 an individual's confidentiality.

- Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

All NHS and Social Services Department are now required to apply these principles and to nominate a senior person to act as a **Caldicott Guardian** responsible for safeguarding the confidentiality of patient information.

Freedom of Information Act 2000

This 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 release of personal information remains protected by the Data protection Act 1998.

The Children Act 2004

The Act provides a legislative spine for the wider strategy to improve children's lives. This covers the universal services which every child accesses, and more targeted services for those with additional needs. The overall aim is to encourage integrated planning, commissioning and delivery of services as well as improve multi-disciplinary working, remove duplication and increase accountability. There is a duty to cooperate between relevant partners in the making of arrangements to improve the well being of children.

Other relevant legislation

Criminal Procedures and Investigations Act 1996

Regulation of Investigatory Powers Act 2000

Health and Social Care Act 2001 (Section 60)

Homelessness Act 2002

Safeguarding Vulnerable Groups Act 2006

Education Act 2002

Mental Capacity Act 2005

Local Government Act 2000

There are statutory restrictions on passing on information linked to:

NHS (Venereal Disease) Regulations 1974

Human Fertilisation and Embryology Act 1990

Abortion Regulations 1991

Further Guidance

HM Government Publications:

Information Sharing: Guidance for practitioners and managers

Information Sharing: Pocket Guide

Available at www.teachernet.gov.uk/publications or Phone: 0845 60 222 60 for copies

Appendix II

INFORMATION SHARING AGREEMENT

This agreement is to be used in conjunction with the Inter Agency Information Sharing Protocol and complies with all the guidance therein.

1. Parties to this agreement

Agency Name	
Address	
Responsible Manager	
Contact Details	
Source/Recipient?	
Authorised Signatory/Date	

Agency Name	
Address	
Responsible Manager	
Contact Details	
Source/Recipient?	
Authorised Signatory/Date	

Agency Name	
Address	
Responsible Manager	
Contact Details	
Source/Recipient?	
Authorised Signatory/Date	

Date of Agreement	
-------------------	--

2. Specific purpose(s) for which the information sharing is required

--

3. Type and status of information shared

Is the information 'person identifiable'?	Yes/No
Has explicit consent been given and recorded?	Yes/No
Has implied consent been recorded?	Yes/No
Is the subject aware that sharing will take place?	Yes/No
Is the information anonymised?	Yes/No

4. Legal basis for sharing where no consent given

--

5. Information Items shared

This list must be comprehensive and include ALL data items that are to be shared

6. Information Transfer Method

All parties to this agreement are responsible for ensuring that appropriate security and confidentiality procedures are in place to protect the transfer and use of the shared, person identifiable information.

Regular flow (specify frequency)	
Ad hoc	

More than 50 items per flow	
Less than 50 items per flow	

Give full details of how the transfer will be made and what security measures will be in place e.g. encryption, registered post

Face to face	
Telephone	
Safe haven fax (or faxed following procedure)	
Electronically (state method)	
Royal Mail	
Secure Courier	
Encrypted removable media	
Other	

Has a risk assessment been carried out on the chosen methods of transfer?	Yes/No
--	---------------

What are the identified risks?	
---------------------------------------	--

7. Audit and Review

Agency Name	
Address	
Responsible Manager	
Contact number	
Review Date	

APPENDIX III

INTER-AGENCY PROTOCOL FOR SHARING INFORMATION

MEMORANDUM OF AGREEMENT

The signatory agencies to this agreement endorse the vital importance of the sharing of information between the agencies to support the provision of effective and efficient services to the populations of the local area.

The signatory agencies are committed to working in partnership on this and future information sharing activities and recognise that without such sharing the increasing amount of initiatives requiring a multi-agency approach cannot be fully achieved.

The signatory agencies accept and support the principles and processes identified in the Inter-Agency Information Sharing Protocol.

The signatory agencies are committed to ensuring that their agencies have in place the appropriate policies, procedures and training to maintain the security and confidentiality of shared information.

The signatory agencies are committed to the monitoring and review of the information sharing processes arising from this protocol.

The signatory should be either the Chief Executive or the Caldicott Guardian of the organisation.

INTER-AGENCY INFORMATION SHARING PROTOCOL

I (name of signatory)

On behalf of (name of agency/authority)

Hereby agree to the following:

- ◆ To subscribe to the principles contained within the Protocol
- ◆ To work to the principles contained within the Protocol
- ◆ To ensure that the Protocol is fully implemented within the agency/authority and all relevant staff are trained in the principles and legal requirements
- ◆ To contribute to the development of trust between the signatory agencies by working within the framework of the Protocol

Signature Name

Position Date

Appendix IV

Current Signatories as at February 2009

Calderdale and Huddersfield NHS Foundation Trust
Calderdale Metropolitan Borough Council
Calderdale Primary Care Trust
Kirklees Metropolitan Council
Kirklees Primary Care Trust
Mid Yorkshire NHS Trust
National Children's Centre
Oakdale Group
Probation Service
South West Yorkshire Mental Health Trust
Wakefield District Primary Care Trust
Wakefield Metropolitan District Council
West Yorkshire Fire Service
West Yorkshire Police Force
Yorkshire Ambulance Service