Multi-Agency Protocol for Information Sharing in Bedfordshire and Luton

Alison Johns
Bedfordshire Shared Services

7-Nov-03
PP5

Policy Name:	
Date of Issue:	
Contact:	
Author:	
Version No.	
Date of Review:	
Document Number:	
Approved by DMT:	

ADULT SOCIAL SERVICES

Contents 1

Background and Summary

Introduction

This protocol has been developed through a partnership between health social care and criminal justice agencies in Bedfordshire and Luton in order to provide a framework for the sharing of information locally within the framework of the Law and government policy

Why is a Protocol Needed?

Government Policy
Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services. This is made clear in a number of documents including the NHS Plan," Information for Health" and the National Service Frameworks.

Public Safety
A number of recent tragedies including the Climbie and Soham cases have highlighted the risks from the failure of agencies to share information on people known to be a risk to the public and those felt to be at risk. Guidance is therefore vital to advise staff how to share information as needed with due regard to the framework of current Data Protection Legislation.

Technological Development
The need for Protocols to govern the sharing of personal information has increased in recent times also due to the speed with which personal information can be transferred from one organisation to another via electronic communication.

Much of the information that needs to be shared involves personal details about service users and their needs.

What is the Protocol?

The Protocol is an over-arching framework for sharing information between health, social care, the police, probation and other agencies in Bedfordshire and Luton. It focuses on requirements for sharing personal information about service users. The Protocol:

- Clarifies the legal background on information sharing
- Outlines the principles that need to underpin the process
- Provides practical guidance on how to share information in a series of supporting Procedures
- Provides a framework within which organisations can develop Information Sharing Agreements (ISAs) for specific areas of service
- Includes arrangements for monitoring and reviewing the use of the Protocol and for responding to breaches

Specific Information Sharing Agreements (ISAs)
Individual Services agreements will specify the specific legislation and operational procedures for implementing the protocol in individual service areas. Where integrated information systems are being developed these arrangements may need to be fairly detailed but will not need to include the general legal information contained in the protocol (Appendix 4).

What are the Objectives of the Protocol?

For the citizen:

- a faster service if information can be found more quickly
- less bureaucratic service not having to repeat information
- The safety of the public if relevant staff have access to current information
- the provision of co-ordinated care
- improved access to records held by agencies

For the Member Agencies:

- Empowering staff by providing ready access to customer information
- Safer for case responsible worker as access to appropriate information on customer
- Enabling staff to meet statutory duties across agencies
- Improved data integrity and information quality to enable better management of the quality of performance
- Allows staff to be flexible and responsive to changes in the situation of service users and carers
- Enables partnership and shared practice between agencies
- Managing risks to staff and organisation more effectively

Risk Management
In developing this protocol agencies are seeking to minimise the risks from the failure to share information appropriately.

These risks include:

- Reluctance to share information in life - threatening situations because of uncertainties about current legislation and guidance.

- Informal arrangements to share information that may not comply with guidance or the law leaving individuals and the organisations they work for at risk of possible legal action.

- Failure to share demographic and service based information needed for effective joint commissioning and management

Legal Framework
Although the Protocol itself is not contractually binding it is based on legislation and common law (Appendices 1, 3). All member agencies have a duty to comply with the law which is regulated by the Information Commissioner. The aim of the protocol is to help

set good practice standards in order to fulfil any duty of care which exists, in relation to the sharing of personal information about service users or staff details that may be necessary to be recorded for the purposes of client care.

The Government has also emphasised the importance of security and confidentiality in relation to personal information and has strengthened the legislation and guidance in this area in particular through the 1998 Data Protection Act and Caldicott guidance (Appendix 1). Guidance from the NHS Information Authority 'Information for Life' additionally emphasises the need to create a *confidentiality culture* which includes understanding confidentiality and consent issues from a patient perspective (Appendix 2).

The Caldicott report (Appendix 1) requires that health organisations should draw up and implement protocols in order to protect patients' confidentiality as well as to facilitate the transfer of information between practice organisations on a 'need to know' basis for justifiable purposes. These standards have now been extended to Social care organisations. Locally it has been agreed that all member organisations broadly share the Caldicott principles in addition to their own internal procedures

Public sector data-sharing is regulated by a number of other overlapping statutes including:

- the law that governs the actions of public bodies 'administrative law'
- The Human Rights Act 1998 and the European Convention on Human Rights;
- The common law tort of breach of confidence; and
- European Union Law

Implementation
In certain circumstances, where there is a strong public interest justification then public sector bodies can lawfully disclose personal information to the police or other agencies, for example, where the information suggests that a serious criminal offence has been committed or where disclosure may reduce the risk of children being harmed.

The protocol will seek to clarify the law generally and exemptions in more detail, however, it may not always be easy to determine whether data-sharing is, or is not permissible and specialist legal advice may be necessary in some cases (Appendices 1, 2).

Information Sharing with Bedfordshire Police
While Bedfordshire police agree to the principles contained within this protocol there may be occasions when information exchange cannot take place due to other legislation or binding agreements under which Bedfordshire police are bound by.

The Information Sharing Protocol

Section 1 – Introduction

1.1 Scope

This Protocol is an agreement between the agencies detailed in section 1.2 to govern the sharing of personal information about service users and facilitate the development of information sharing agreements. On occasions the legitimate sharing of personal information about staff may be necessary which will be covered by the same principles and culture of confidentiality covered by this protocol.

1.1.1 **Information needing to be shared:**

The protocol focuses primarily on the sharing of personal and sensitive data about people using health, social care and associated services commissioned by the partner agencies listed in Section 1.2. Definitions of the terms “personal data” and “sensitive data” are found in the Data Protection Act (1998). The Protocol also refers to “private” information in relation to the Human Rights Act 1998 and “confidential” information (Appendix 3).

The sharing of information is covered for any purposes listed in section 2.1, comprising the common principles and procedures to be adopted wherever and whenever these organisations share information for these purposes.

A framework is provided for information sharing in Bedfordshire and Luton. It will be activated through Information Sharing Agreements (ISAs) for specific areas of service between partner agencies. Each ISA will set out the detailed arrangements relevant to that particular application and will need to be fully compliant and consistent with this Protocol.

1.2 Parties to the Protocol

The following organisations are parties to the Protocol

Bedford Hospital NHS Trust
Bedford NHS Primary Care Trust
Bedfordshire and Luton NHS Community Trust
Bedford Borough Council
Bedfordshire Heartlands NHS Primary Care Trust
Bedfordshire Strategic Health Authority
Bedfordshire & Hertfordshire Ambulance and Paramedic NHS Trust
Luton & Dunstable Hospital NHS Trust
Luton Borough Council
Luton NHS Primary Care Trust
Bedfordshire Police
National Probation Service-Bedfordshire
Bedford NHS Primary Care Trust also aims to explore the avenue of improving links with those responsible for the health of inmates at Bedford Prison for information sharing purposes.

Section 2 - Principles

2.1 Purposes for which information may be shared

This Protocol applies to the sharing of information between agencies for the following purposes:

- Improving the delivery of services
- Protecting people and communities
- Prevention and detection of crime
- Investigating complaints
- Developing inter-agency strategies
- Planning services
- Performance management and audit
- Research relating to clinical or social care objectives

2.2 Principles governing the sharing of information

1. **Commitment to sharing information**
   Partner organisations recognise that multi-agency initiatives require a commitment to sharing personal information about service users in compliance with guidance and legislation

2. **Statutory duties**
   Partner organisations are fully committed to ensuring 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 (Appendix 1)

3. **Caldicott requirements**
   All organisations recognise the requirements that Caldicott imposes on NHS organisations and Social Services Departments. They will ensure that requests for information from these organisations are dealt with in a manner compatible with these requirements (Appendix 1)

4. **Duty of confidentiality**
   It is generally accepted that most (if not all) information provided by service users is confidential in nature. All organisations which 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 doing so. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility

5. **Consent**
   Organisations will seek consent from the service user to share personal information unless there are reasons to do otherwise. If consent is not sought the reasons for this must be fully documented. Where consent to disclose information is requested, the service user will be made fully aware of the information it is proposed to share and the purposes for which it will be used,

in accordance with the Fair Processing Code of the Data Protection Act 1998.

If a person is unwilling to give consent, information will only be shared in exceptional circumstances and where there are appropriate statutory grounds for doing so.

6. **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. Relevant staff will be provided with information about these procedures.

7. **"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

8. **Information kept confidential from the service user**
   Where professionals request that information supplied by them be kept confidential from the service user, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on statutory grounds, for example, under the provisions laid out in the Mental Health Act (1983) (Appendix 1) where it may be judged that it is in the clients best interests to withhold certain information or, for example, under the conditions of Schedules 2, 3 of the Data Protection Act 1998 (Appendix 1).

9. **Specific purpose**
   Partners will not abuse information that is disclosed to them under the specific purposes set out in the protocol. Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for the general use of the organisation and can only be used for the purpose for which it was disclosed.

10. **Fact / opinion**
    When disclosing information about an individual, professionals will clearly state whether the information being supplied is fact, opinion, or a combination of the two. The source of the information should also be clearly identified e.g. doctor x opinion

11. **Use of anonymised information where possible**
    Personal information will only be disclosed where the purpose for which it has been agreed to share is clearly necessary. For all other purposes, information about individual cases will be anonymised (App 3).

12. **Access to information**
    People will be fully informed about the information that is recorded about them. 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 within their personal written records. With the persons consent this correction will be notified to any partner agencies currently involved

13. 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

14. Staff awareness

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

- the Protocol
- the confidentiality of information about service users
- the commitment to share information in accordance with this guidance and legislation

15. Disciplinary action

Partner organisations will ensure that contracts of employment and standing orders include reference to the issue of disciplinary action should staff disclose personal information on a basis which cannot be justified on statutory grounds.

Section 3- Operational Procedures

3.1 Adoption of procedures

A key aspect of the Protocol is the adoption by partners of a common standard for procedures for the sharing of information. This is intended to give organisations confidence that when they share information (under Information Sharing Agreements) partner agencies will be operating to a common standard that complies with relevant legislation and guidance. (Partner organisations may already have procedures in place which meet these standards and will want to use these).

3.2 Joint Procedures: Disclosure of Personal Information

3.2.1 Explicit consent should be sought at the earliest opportunity. This should be at the first contact unless the individual is unable, at that time, to fully comprehend the implications or make an informed judgement. If, in the professional judgement of the staff member(s) concerned, it would be detrimental to the health or safety of the person concerned to address these issues at that time, then the reason for not doing so should be recorded and arrangements agreed to complete this process at the first available opportunity.

3.2.2 **Training for Consent Seeking**

The agencies will ensure that those who may have to seek the consent of a person to share information about them, will be competent to present and explain the issues to the individual, to request their consent to share personal information with other agencies and to explain the consequences if consent is not given. Multi- agency training regarding the issues concerning consent seeking and confidentiality to be developed where possible. Each organisation will maintain records of those who are competent to seek consent.

3.2.3 **Informed Consent**

When gaining consent informed consent (Appendix 5) should always be obtained from the individual who is the data subject. Where there is any doubt about the capacity of a person to give consent a specialist assessment of capacity may need to be obtained.

3.2.4 Where a person does not have the capacity to make an informed decision but another person has authority to act as their guardian and take decisions on their behalf, then this situation must be explained to that person. Individual protocols ISA's will identify who is able to take decisions on behalf of the client group concerned.

Where it has been established that a client is able to make an informed decision then the member of staff will first tell the client that:

- Everyone has a right to prevent disclosure about themselves
- It is a requirement of the Data Protection Act 1998 that consent to disclosure of information should only be on an informed basis (Appendix 1, 3).

- The right to prevent disclosure is recognised by the organisation(s) involved. However, the organisation has a responsibility in certain circumstances to take action to prevent harm to an individual or to protect their vital interests. If, in a particular case, the organisation concludes that they have such a responsibility and this constitutes statutory grounds for disclosing information without consent, then they may exercise their right to do so.

3.2.5 **Sensitive Personal Data**
Where Sensitive Personal Data is processed for medical purposes, it is not always necessary to obtain the explicit written consent from the individual although it is advisable to explain the purposes for using the information. (Details of medical exemptions in appendix 3).

A note should be made in the record confirming that discussion has taken place between the individual and one of the NHS Health Services to seek agreement that their personal information can be shared between the agencies signed up to this protocol and used within the remit of the protocol.

3.2.6 Where Sensitive Personal Data is processed for Social Care reasons, it is necessary to obtain the explicit written consent from the individual, unless exclusions apply under relevant legislation (Appendix 1).

3.2.7 **Information Sharing Agreements ISAs**
Individual agreements will specify the circumstances under which professionals may disclose information without consent (Appendix 4)

3.2.8 **Sharing Information with other Agencies**
The client or their guardian should be made aware that information about their case may be shared with other agencies for planning of services. They should be assured that for these purposes personal information is not released but only data that has been anonymised or shared in aggregated form (Appendix 3)

3.2.9 The client or their guardian will also be made aware of any specific records or systems which are maintained to support the purpose for which they are in contact with the organisation (e.g. the log maintained by the child protection coordinator). Each agency will determine how individuals will be informed of the purpose and content of these records, how they are stored, and who has access to them.

3.2.10 the client or their representative will be made aware that their sensitive personal information will only be shared with other agencies for the purposes they have consented to, unless disclosure for other purposes is necessary to protect the vital interests of the service user or the public

3.2.11 Agencies will also make available a copy of the protocol if requested.

3.2.12 the material should be available in a variety of formats and languages. The person, or their legitimate representative, must be given sufficient time and help to access and understand and consider the material provided.

3.2.13 An "Information for the public "strategy to be developed to inform the public of their rights and the requirement for them to give consent as part of the 'confidentiality culture' (Appendix 2)

3.3 Recording Consent

3.3.1 Agencies must have a means by which an individual can record whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure. For health information patients may ask that certain parts will be restricted from normal sharing which will then have 'sealed envelope' access and any risks to the individual from this decision will be explained to them (Appendix 2).

3.3.2 Individuals should be able to prescribe, in respect of all information held by the contact organisation:

- With which organisations information can and cannot be shared with
- What information known to the contact organisation can be shared and what information should remain confidential

These limitations should only be overridden if there are statutory grounds for doing so (Appendix 1)

3.3.3 For sensitive information (as defined by the DP Act 1998) (Appendix 1) which is held by the contact organisation, individuals will be able to prescribe the explicit purposes for which they agree to this information being disclosed to another organisation.

3.3.4 It is recognised that in an urgent or emergency situation it is impractical for existing client records to be studied in detail and amended at that point in time. Therefore an individual must routinely have access to what information is recorded (both manual and computerised) and be given an opportunity to amend or correct any information which is incorrect.

3.4 Disclosure of Information

3.4.1 Unless details of consent are recorded electronically an individual's manual personal case file should always be checked before personal information is disclosed to another agency. Members of staff without access to an individual's case file must check with case holders or their manager before releasing information.

3.4.2 It is essential that the person receiving a request for personal information about a client first checks that a consent form accompanying the request does not contradict any previous consent agreements held in their organisation's case file. Any contradictions must be resolved before information is released by notifying the persons responsible for controlling access to information. Legal advice should be taken if necessary.

3.4.3 Particular care should be taken before sensitive information as defined by the Data Protection Act (1998) is released. Sensitive information should only be

released if its disclosure is critical to the case and explicit consent has been given to its release for that purpose.

3.4.4 When disclosing information about individual clients, organisations must indicate to what extent this information is current, is factual or an expression of opinion and whether it has been confirmed by the client.

3.4.5 It is recognised that in particular investigations (e.g. Adult protection enquiries) the significance of information may not be initially apparent and agencies may put in place procedures which enable them to share all information they hold about the person(s). In this case individual protocols will state that such an agreement has been made and will make explicit the specific arrangements they have put in place to limit the access to such information to those with a need to know.

3.4.6 Organisations will be kept fully informed about the disclosure of information originating from their files, whether it is with or without the consent of the person to whom the information pertains. Accurate records must be kept of what information has been disclosed to whom, the source of the data disclosed, and the date on which it was disclosed and protocols must specify who will be responsible for ensuring that this is done.

3.4.7 **Disclosing information without consent**

- Passing information without consent places both individual staff members and organisations at risk of prosecution. There is also the risk of a compensation order under the Data Protection Act, or damages for breach of confidence/breach of the Human Rights Act Article 8 rights (Appendix 3)

- The disclosure of personal information without consent must be justifiable on statutory grounds and meet one of the conditions of Schedule 2 of the DP Act 1998 (Appendix 3)

- In addition, the disclosure of ”sensitive” information without consent must meet one of the conditions of Schedule 3 of the DP Act 1998 (Appendix 3).

- Each agency will therefore appoint a responsible person or persons with the authority to take decisions in case of emergency situations.

- If in doubt the case should be referred for legal advice and each organisation will ensure that the responsible staff know how and who to contact for legal advice.

- If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Individual protocols will specify the person(s) responsible for ensuring this happens.

- Organisations will nominate contacts for the receipt of personal and sensitive information. These contacts will be responsible for ensuring that information

is restricted to those who need to know it for the purposes agreed. Individual protocols will set out the contacts agreed for the purposes integral to that protocol.

- Recipients of the information will be made aware that it has been disclosed without consent and will put agreed security procedures in place.

- A record of the disclosure will be made in the client's file and the client or their guardian informed

3.4.8 **Staff Guidance on Consent Seeking**
To support staff, each organisation will put in place procedures which give clear guidance on:

- The need to seek consent and the consequences of not doing so

- Who is trained to seek consent and how their involvement should be initiated

- Who is able to take a decision on behalf of another person

- The circumstances under which information may be disclosed without consent, who can authorise this disclosure, how the authority should be requested and what records must be kept of this process

- The procedures for recording and storing consent to share information whether full or limited consent and what the relevant procedures should then be in either circumstance.

3.4.9 Individual protocols will include a date by which all parties to the protocol will have these procedures in place and will set out how progress in implementing them will be monitored

3.5 Access and Security Procedures

- Details of how "need to know" access will be determined will be through the use of judgement of designated trained staff.

- All organisations will have procedures to be able to identify the correct individual, about whom there is an information request, using a common identifier, if available.

- Precautions will be made to ensure that information which identifies individual clients and/or patients is transferred and shared in a secure manner ensuring 'safe haven'.

- Where fax transfer of information is unavoidable the multi-agency procedure for secure transfer by fax will be followed.

- Electronic transfer of personal information will only be permitted on a person-to-person basis across networks or by disc delivered directly to the intended

recipient. Information security standards (BS7799) and the Caldicott principles will apply.

- For urgent requests for information made or provided via the telephone or face-to –face the multi-agency code of conduct for transferring and sharing information verbally will be followed.

- Written communications containing personal information should be transferred in a sealed envelope marked “Personal and confidential – to be opened by recipient only” and addressed by name to the designated person within each organisation. Dispatch of such requests should be made known to the recipient. Individual protocols will have varying security markings and arrangements depending on the sensitivity and subsequent classification of the information.

- Record keeping systems will enable secure management & storage, where information is kept, according to relevant legislation, including how long the information may be stored for and arrangements for notification of intention to destroy information.

3.5.1 **Disciplinary Procedures in case of Breaches of the Protocol**
Each member organisation will specify what disciplinary action or legal proceedings may be taken against the individual in case of a serious or intentional breach of information. Significant breaches will be notified to the partnership.

3.5.2 **Restrictions on the use of Statistical and Anonymous Data**
Organisations in receipt of statistical data derived from client records of partner organisations must request permission from the originating organisations (the data owner) if they wish to use that information for any purpose other than that for which the information was originally provided.

3.5.3 Individual protocols should also specify arrangements for the approval of the wider use or publication of case studies based on material collated for the specific purposes covered by the protocol

Section 4 - Implementation of the Protocol

4.1 Consent Form

A multi- agency consent form to be developed to be used in appropriate circumstances. The consent form should be stored in the individual's personal record file and the file marked to indicate that consent forms are present. A copy of the consent form should be given to the individual.

4.2 Limitation of Consent

If a person limits the disclosure of information in any way then this must be flagged by being recorded both on the consent form and on their records in an obvious way so that the limitation of the consent is immediately noticeable from the file. Information which is held with this limitation should be stored so that access can be appropriately controlled. This limitation of consent should be recorded whether or not a decision is taken to disclose without consent.

4.3 Structures and responsibilities

The key areas of responsibility in relation to the protocol are summarised below

Organisation	Responsibility
Bedfordshire & Luton Information Partnership	Commissioning the protocol
Chief Officers / Boards of each of the partner organisations	Formal Adoption
Bedfordshire & Luton Information Partnership	• Dissemination arrangements • Implementation within organisations • Monitoring implementation • Monitoring compliance • Adjudicating on breaches • Approval of major amendments

4.4 Raising awareness & disseminating the Protocol

The protocol raises awareness of the key information sharing issues and provides detailed procedural guidance. Training material will be made available to support implementation. This will help organisations to ensure that staff are aware of these key issues and have confidence in the process of sharing information with others.

4.4.1 Following formal approval, the protocol will be disseminated to all staff who will be directly involved in its implementation. Copies will also be available for other staff and will be made available to the Library Service, on the internet, and to other appropriate organisations on request. All partners will make copies available to service users, carers and members of the public.

4.4.2 Training materials will be made available to support training programmes.

4.5 Maintaining Contact Details

4.5.1 All organisations will maintain a list of staff who are authorised to seek consent and specify how the list will be maintained

4.5.2 Organisations will provide the names and contact details of members of staff to whom requests for information should be directed

- who can authorise disclosure in respect of individual protocols
- how to access legal advice
- who is authorised to receive confidential information

4.6 Monitoring arrangements

The information Sharing Steering Group will be responsible for overseeing the monitoring and review process. Monitoring will be carried out by:

1. Following adoption of the protocol, lead members will provide confirmation that procedures have been implemented within their organisation in accordance with the protocol
2. Complaints received by organisations relating to information disclosure will be analysed to determine whether they relate to a breakdown or an inadequacy of the protocol
3. Where individual ISAs specify the provision of statistics and reports, lead members will be asked to confirm receipt of these
4. All reported breaches of the protocol will be followed up in accordance with Procedure

4.7 Review arrangements

The review process will be carried out in accordance with Procedure.

1. During the initial six months of implementation, use of the protocol will be monitored and issues/ problems arising will be noted. Changes to the protocol will only be considered during this period if the Bedfordshire Information Partnership consider the issue to be significant
2. The first formal review will be held six months after the date of implementation. Reviews will then be carried out annually unless legislative changes require more immediate action
3. One month prior to the review date, all parties to the protocol will be asked to submit feedback on the use of the protocol and put forward proposals for amendments. Legal advice will be obtained in relation to any proposed major changes

Section 5 – Adoption of the Protocol

5.1 Undertaking

The parties to the protocol agree that the procedures detailed in the document provide a secure framework for the sharing of information between their respective organisations in compliance with their statutory and professional responsibilities

As signatory we undertake to:

- Facilitate the sharing of information wherever such sharing is lawful
- Ensure that staff adhere to the procedures and arrangements set out in the protocol
- Provide evidence, when requested, that agreed procedures and arrangements have been implemented
- Ensure that all agreements established between our agencies for the sharing of information are consistent with the protocol

5.2 Signatures of the Parties to the Protocol

Organisation	Name and position of signatory	Signature	Date
Bedford Hospital NHS Trust			
Bedford NHS Primary Care Trust			
Bedfordshire and Luton NHS Community Trust			
Bedford Borough Council			
Bedfordshire Heartlands NHS Primary Care Trust			
Bedfordshire Strategic Health Authority			
Bedfordshire & Hertfordshire Ambulance and Paramedic NHS Trust			
Luton & Dunstable NHS Hospital			
Luton Borough Council			
Luton NHS Primary Care Trust			
Bedfordshire Police			
National Probation Service-Bedfordshire			

Appendix 1

Legislation

The Caldicott Report – "Protecting and Using Patient Information "

Principle 1 - Justify the purpose
Every proposed use or transfer of personal identifiable information within or from an organisation should be clearly defined and scrutinised with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 - Don't use personal identifiable information unless it is absolutely necessary
Personal identifiable information items shall not be used unless there is no alternative

Principle 3 - Use the minimum necessary personal identifiable information
Where use of personal identifiable information is considered to be essential, each individual item of personal information should be justified with the aim of reducing identity.

Principle 4 - Access to personal identifiable information should be on a strict need to know basis
Only those individuals who need access to personal identifiable information should have access to it and they should only have access to the personal information items that they need to see

Principle 5 - Everyone should be aware of their responsibilities
Action should be taken to ensure that all staff who handle personal identifiable information are aware of their responsibilities and obligations to respect confidentiality

Principle 6 - Understand and comply with the law
Every use of personal identifiable information must be lawful.

Data Protection Act 1998

The purpose of the Act is to protect personal information being used for purposes other than that for which it has been collected for and states that data should be:

- Obtained and processed fairly and lawfully
- Obtained for one or more specified purposes
- Accurate and where possible kept up to date
- Kept for no longer than is necessary
- Processed in accordance with the rights of the data subject
- Stored using appropriate measures against accidental loss or destruction or damage to personal data
- Data should not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects

The Act refers to “personal data” which means which relates to an identifiable living individual and “sensitive personal data”. trade union membership, physical or mental health, sexual life, commission or alleged commission of offences and criminal convictions or proceedings. For medical purposes, for example, obstetric history may be relevant to share between professionals.

Human Rights Act 1998

Under the European Convention of Human Rights, individuals have the right to respect for a private and family life (article 8). There should be no interference with this right by a public authority unless it is in accordance with the law and necessary for the prevention of crime and disorder, for the protection of rights or morals, or for the protection of the rights and freedoms of others. Any interference of the right must be proportionate.

Common Law

The unwritten law of England and Wales that is embodied in judicial decisions as opposed to statute or the law enacted by parliament

Mental Health Act (1983)

Information such as diagnosis may be withheld from the individual where it is judged that disclosing the information would be likely to cause harm

Crime and Disorder Act (1998)

Authorises any person to provide information to the police, local authorities, probation authorities, health authorities in connection with the purpose of that Act.

Appendix 2

Other Guidance

a) Information for Life NHS Information Authority (2001)
Caring for Information Model for the Future

Patients can ask that certain parts of their health information be restricted from normal sharing. Information that a patient restricts will not be accessed by anyone without the patient's permission, subject to limited exception. Patients wanting to limit sharing are provided with the means to do so (a 'sealed envelope')

Draft Guidance on Public Sector Data- Sharing Produced by the Lord Chancellor's Department May 2003

Appendix 3

Definition of Terms

Common Law duty of confidence
In general, any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information.

Consent
The Data Protection Act defines the Data Subjects consent as:" any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"

The fact that the data subject must signify their agreement means that there must be some active communication between the parties. Agencies **cannot** infer consent from non-response to a communication of from a customer's failure to return or respond to a leaflet

Informed Consent
Informed consent means that there has to be some active communication between the two parties regarding the purposes of their data and a verbal agreement must be gained before the processing can continue

Explicit consent
As for informed consent but with a signature by the data subject against the requirements.
Is also termed informed consent particularly in medical procedures.

Data
Electronic or highly structured paper records as set out in Section 1 of the Data Protection Act 1998

Anonymised Data
Statistical information only

Psuedonymised Data
Anonymised for recipient, but traceable for sender

Privacy
The meaning of 'privacy' or 'private life' is not precisely defined for the purposes of the law. Private matters include details about a person's home, family, religion, health or sexuality

Sensitive personal data
Personal data about ethnic or racial origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of offences and criminal convictions or proceedings. For medical purposes, for example, obstetric history may be relevant to share between professionals.

Appendix 4

Individual Service Level Agreements

This is the proposed structure for an ISA

- The data to be provided by each organisation
- The start date, frequency, format and quality
- Procedures for the routine transfer of anonymous data
- Procedures for routine transfer of, or access to, patient-identifiable data
- Procedures for reviewing the continued need for the transfer
- Procedures for dealing with requests for additional data items
- Procedures for submitting a request for non-routine transfer of or access to information
- Agreements on the quality and timeliness of data

Appendix 5

Procedures to enable Informed Consent

In order to ensure that consent to the sharing of personal information is informed; all agencies will be able to explain:

- The rights of individuals under the Data Protection Act 1998, particularly in relation to sensitive information;
- Procedures in place to enable clients/patients to access their records
- Procedures which may be initiated when a member of staff suspects that an adult or child has been or is at risk of abuse, including details of who information will be shared with at each stage, what information will be shared and how the information will be used.
- Circumstances under which information may be shared without consent and the procedures which will be followed
- The complaints procedures where an individual believes information about them has been inappropriately disclosed
- How the information about an individual will be recorded, stored and the length of time it will be likely to be retained both by the point of contact agency and the agencies to whom they may disclose that information.
- The length of time for which consent to particular disclosures is valid