

# **Information Sharing Agreement**

---

Principles, purposes and organisational responsibilities required for information sharing

<b>Document change history</b>		
Document status: <b>final</b>		
<b>Version</b>	<b>Date</b>	<b>Comments</b>
1.0	February 2003	Issued to stakeholders for review and comments. Agreed in principle by Gloucestershire Caldicott Guardians
2.0 – 2.5	March - May	Reviewed and updated
2.6	May 2003	Comments incorporated from stakeholder consultation prior to issue for signature to organisations in 'Avon'
2.6	July 2003	Agreed by Gloucestershire Caldicott Guardians

## Purpose & Overview:

To facilitate the lawful exchange of personal & sensitive data, in any form, within and between organisations for notified and defined purposes, respecting the rights of individuals set out in legal acts and common law. It covers the sharing of information that is in any way, personally identifiable or sensitive about individuals that are living. The principles may be used as the basis for any policy area that requires information to be shared, such as protection of vulnerable people & children. It is intended to support, not replace such 'specialist area' policy and process.

## Categories of Information:

Records containing any of the following items should be treated as sensitive and/or identifiable and appropriately handled in line with principles and responsibilities defined below.

Personal Information	Sensitive Information
• Forename, Surname or Initials	• Racial or Ethnic origin
• Date of Birth	• Political Opinion(s)
• Gender	• Religious Belief or other beliefs of a similar nature
• Address details (especially Postcode)	• Trade union membership
• Identity Number (e.g. NHS, NI Numbers)	• Physical or mental health or condition, nature of abuse
• Occupation	• Sexual life
	• Offences committed or alleged offences, Court proceedings

## Principles for recording, using and sharing information (including Caldicott):

Organisations and all staff employed by them must:

- Justify and, if at all possible, document the purpose for recording and/or sharing information
- Only use and share information when absolutely necessary
- Use the minimum information required for the purpose - anonymising or removing as much personal/sensitive information as possible
- Only access information with consent or on a strict 'need to know' basis
- Ensure awareness and understanding of everyone's responsibilities to maintain confidentiality including understanding & complying with law, (inc. Data Protection, Human Rights – right to privacy & common law of confidentiality)
- Information shared can only be used for the purpose(s) originally agreed at the time of disclosure. If later required for another purpose, the recipient must confirm appropriateness with the supplier.
- Any information disclosed to an organisation will be classified as their data and they become data controllers of that information.

## Fair & lawful processing (including consent):

Obtaining, holding, using and sharing personal/sensitive information will be based on 'informed' consent. Where required by law and in every other possible circumstance this will be 'explicit informed consent'.

However there are situations where this is not always possible, i.e. where the view of the senior professional involved with the individual, is that the subject is substantially incapacitated and is unable to consent. In such circumstances staff will be required to act in the 'best interests' of the individual.

The areas where explicit consent is required are:

- Involvement in or use of identifiable information for (or shared for) teaching & research
- Taking & sharing audio/visual recordings (photos, video, audio etc) which in anyway identify an individual which may or will be used for purposes other than direct care of the individual
- Transfer of information to solicitors and insurance companies
- Where no other condition under Data Protection Act Principle 1, schedule 3 can be met
- Where information is to be transferred for purposes not identified in this protocol

In exceptional circumstances, such as where the subject is un-contactable and there is a matter of urgency, 'implied informed consent' can be used for the sharing of information, provided subjects are generally informed of the uses and disclosures of their information and given opportunity to object (see Organisational responsibilities).

Information can be shared, under specific conditions, without consent where there is a legal requirement (inc. Road Traffic, Mental Health & Children Acts) or it is justified to be in the substantial public interest or best interest of the individual, with reference to common law of confidentiality and Human Rights Act.

Operational policy and procedures based on this agreement must detail when information can be shared without consent, by reference to public/best interest justification, other legal duties/powers and where relevant conditions under schedule 2 (personal information) and schedule 3 (sensitive information) of the Data Protection Act can be fulfilled. Organisations must seek advice from Data Protection Officers, Caldicott Guardians and, if required, legal advice.

### Organisational responsibilities (including Data Protection Compliance):

- Organisations must actively inform individuals of how their information may be used and to whom it may be disclosed. It must highlight their rights to access, withhold and correct information and provide details of the process for individuals to access their records.
- Organisations must complete and maintain a Data Protection notification detailing all sources, subjects, purposes and disclosures relevant to their business and partnerships under any agreement.
- Organisations must maintain the accuracy and clarity of data they supply under the agreement to aid usefulness and consistent interpretation. Where necessary, partner organisations will be informed of any changes to the data they have received and also notify the source of any error they discover.
- Organisations must maintain the confidentiality of data in any form, during collection, transmission and storing with appropriate security arrangements, moving to compliance with ISO17799.
- Organisations will apply relevant regulations to the retention & disposal of records, only keeping information for as long as is necessary in relation to the original purpose(s) for which it was collected.
- Organisations will ensure all relevant staff are aware of, understand and comply with these principles and organisational policy on the collection and uses of information, supported by terms of employment
- Organisations will ensure that any 3<sup>rd</sup> parties providing a service to them agree and abide by these principles by inclusion in contracts/agreements.
- Organisations will have at least basic processes/systems for recording wishes/restrictions on information expressed by individuals.

### Purposes for which information can be shared:

In any sharing of information the purpose must be in line with legitimate activities undertaken by an organisation in providing a service to the public, set out in an organisation's legal powers (vires).

• Delivering care and treatment	• Assessment for treatment and services
• Assuring and improving the quality of care / treatment	• Monitoring and protecting public health
• Managing and planning services	• Contracting for services
• Auditing accounts	• Risk management
• Investigating complaints and potential legal claims	• Teaching and training
• Statistical analysis	• Research and audit
• Where emotional, physical, sexual, psychological, financial (material) or discriminatory abuse or neglect suspected, crime committed or regulations breached.	• Ensuring holistic assessment of vulnerable children's development needs or peoples parenting capacity
• Sharing information to match children appropriately with carers	• Equipping the courts with the required information

### Review & compliance:

This set of principles will be reviewed every twelve months, or at request of any signatory organisation. Organisations will complete the attached explanatory & compliance statement detailing how they are undertaking their responsibilities. These will be made available to any partner organisation on request.

### Processes for information sharing:

Each initiative claiming support of this agreement is responsible for creating procedure documentation detailing how information will be shared securely, and how the principles have been applied including how sharing can be audited.

### Indemnity:

In consideration of the provision of information in accordance with the agreement all partner organisations agree that an individual partner will indemnify any other persons or authority that they share information with (**signatory list to be published to all organisations**) against any liability, losses, claims or proceedings, cost charges and expenses (including legal fees) which may have been incurred by such person or authority as a result of the provision of such information by the partner organisation. The indemnity does not apply:

- a) Where the liability arises from information supplied which is shown to have been incomplete or incorrect, unless the person or authority claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part or on the part of any other person or authority supplying the information;
- b) Unless the person or authority claiming the benefit of this indemnity notifies the sharing organisation within 14 days of any action, claim or demand to which this indemnity applies, or permits the sharing organisation to deal with the action, claim or demand by settlement or otherwise and renders all reasonable assistance in doing so. If partner organisations cannot agree how to conduct an action, claim or demand then the partner organisation who is funding the defence of the claim and will ultimately be responsible for the payment of any damages, costs or related expenses shall conduct the matter as it in its reasonable opinion thinks fit
- c) To the extent that the person or authority claiming the benefit of the indemnity makes any admission, which may be prejudicial to the defence of the action, claim or demand.
- d) If the discloser supplies information to the disclosee and the disclosee then uses the information otherwise than in accordance with this agreement, the discloser shall not be liable to the disclosee irrespective of whether or not the information supplied was correct or complete
- e) If a discloser supplies information to the disclosee and the disclosee then uses the information otherwise than in accordance with this agreement, then (except where (f) applies) the disclosee shall indemnify the discloser and keep the discloser indemnified against all actions and claims whatsoever arising from the use of such information
- f) Where the discloser supplies inaccurate or materially incomplete information (whether knowingly or otherwise) to the disclosee and the disclosee uses that information otherwise than in accordance with this agreement, each partner organisation shall indemnify the other against all actions and claims resulting from such use arising from its failure to supply or use the information in accordance with this agreement.

Signed:

Organisation:

Date:

(Chief Executive Officer and/or delegate – such as Caldicott Guardian)

## Organisational compliance statement template (inc explanatory information)

This document sets out required activities for organisations to comply with their responsibilities under the terms of the Information Sharing agreement. These responsibilities are based around the legal framework of the Data Protection Act, the Human Rights Act and common law of confidentiality. Each signatory organisation is required to insert brief notes on activity relating to the identified responsibilities:

### Organisational responsibilities (including Data Protection Compliance):

- Organisations must actively inform patients/service users of the uses to which information about them may be put and to whom it may be disclosed. It must highlight their rights to access, correct and withhold information and provide details of the process for individuals to access their records.

*Minimum activities for compliance include the provision of leaflets with basic details covering the criteria above, supported by identified processes for individuals to make further enquiries, such as contact details for staff handling requests. Other forms of communication with subjects including processes to gain explicit consent are also worth stating, whether this is by specific signatory of the subject to a form, or by verbal questioning during care and treatment (that may or may not be noted):*

- Organisations must complete and maintain a Data Protection notification detailing all sources, subjects, purposes and disclosures relevant to their function and partnerships under any agreement.

*It is mandatory that each partner is registered and that the registration reflects the purposes, sources, disclosures and subject that are elements of the information sharing agreement. In most cases the purposes notified will include: Health Administration & services, social services activity, research, crime prevention and public health*

- Organisations must maintain the accuracy and clarity of data they supply under the agreement to aid usefulness and consistent interpretation. Where necessary, partner organisations will be informed of any changes to the data they have received and also notify the source of any error they discover.

*Please detail any relevant elements of policy/procedure relating to data quality and record creation that aids clarity and consistency. This may include education programmes for staff, operational checks with patients/service users at point of contact (i.e 'please confirm your address'), system specifications for mandatory fields/acceptable values and regular data integrity checks run and/or audits undertaken. For NHS organisations this should include statement regarding 'Data Accreditation'.*

- Organisations must maintain the confidentiality of data in any form, during collection, transmission and storing with appropriate security arrangements, moving to compliance with ISO17799.

*ISO1 (BS) 7799 is the standard for Information Security. Compliance is currently unrealistic, but recognition of moving towards it is required, even if there is no formal analysis programme in the organisation at present. Organisations must confirm the following policy controls as a minimum:*

- *Physical access controls and secure location of equipment (PCs, faxes etc) and information are implemented appropriately for the relevant setting and reviewed at least periodically.*
- *Confidential information transmitted is marked as such (via fax headers, envelopes etc) and only sent when necessary, noting NHS organisations will not send confidential information outside the NHS via email without encryption*
- *Access to computer systems is controlled via usernames and passwords*
- *Identity and authority of requestor(s) are checked and verified by appropriate procedure (callbacks via switchboards when information requested prior to transmission)*

- Organisations will apply relevant regulations to the retention & disposal of records only keeping information for as long as is necessary in relation to the original purpose.

*HSC 99/053 defines retention and disposal periods for records in the NHS. NHS Organisations should confirm they accept these and they are in the process of implementing policy and procedure relating to them. Similar regulations detailing time periods for retention in other sectors should be referenced appropriately. Organisations without regulations should detail relevant activity to decide on length of retention, in line with Data Protection Act principle of 'not keeping information for longer than necessary'. All organisations should give brief detail of disposal policy/procedure (i.e. confidential waste bins/collections)*

- Organisations will ensure all relevant staff are aware of, understand and comply with these principles and organisational policy on the collection and uses of information, supported by terms of employment

*Please detail any activity related to training for staff in relation to confidentiality, quality and security of information. The minimum acceptable level is induction training for all new employees. Messages delivered as part of integrated training in the use of systems or particular operational policy should also be highlighted. Specific training on data protection/confidentiality for key staff should be encouraged. Staff must be bound by terms of employment relating to handling confidential information.*

- Organisations will ensure that any 3<sup>rd</sup> parties providing a service to them agree and abide by these principles by inclusion in contracts/agreements.

*Please confirm that it is organisational policy that contracts with suppliers that handle personal/sensitive information in anyway contain at least basic confidentiality and information security clauses incorporating agreement that information accessed as part of the operation of the contract will be kept confidential and the supplier accepts liability for any breach of confidentiality where they are found to be at fault. Whilst it is likely not all contracts will contain relevant clauses, it is required that this is organisational policy for all new contracts.*

- Organisations will have at least basic processes/systems for recording wishes/restrictions on information expressed by individuals.

*Such systems are not currently common place, and there are general cultures of confidentiality, however individuals may express specific instructions and the organisation must have at least informal processes in place to record such instructions either in paper records or computer systems (ideally both). Overtime these will move to formal processes.*

**Completion:**

Statements should be clear and concise. Large amounts of detail are not required. Completion by the Organisation's nominated Data Protection Officer where appropriate.