Multi-Agency Information Sharing Protocol

Policy Statement approved by:	**B&NES LSAB (approved)**		
Implementation Date:	**June 2014**		
Review Date:	**June 2017**		
Status:	**Review of draft**	**Version no:**	**2.0**

Distribution:

Releasing and issuing of this agreement is subject to the terms and conditions of the Freedom of Information Act 2000.

Version Control:

Issue	Date	Author	Summary of Change
0.1	**05/11/2013**	**Alan Mogg (Team Manager, Safeguarding Adults and Quality Assurance, B&NES Council) NB: this is a revision of an original document dated April 2010 produced by Glyn Young, Information Governance Manager, NHS B&NES)**	**Draft document issued for comment**

Table of Contents

1.0 Introduction

1.1 The aim of this agreement is to establish a common set of key principles and standards to be used by all professionals working with the Multi Agency Safeguarding Adults Policy. The partner organisations of the Bath and North East Somerset Local Safeguarding Adults Board ('B&NES LSAB') who are party to this agreement recognise that they work in a multi-agency environment and that the exchange of information about individual service users is essential to the provision of that service. The adoption of a multi-agency approach to address service issues therefore includes a commitment to ensuring such information is shared, albeit in a manner which is compliant with their statutory responsibilities.

1.2 As well as identifying the standards and principles, it is intended to provide practitioners with practical guidance to enable them to share information confidently and appropriately and legally. It is not intended to put barriers in the way of information sharing.

1.3 It is intended to provide a common approach to, and understanding of, the responsibilities of all professionals when seeking to share information about vulnerable adults who may be at risk from abuse.

1.4 The key principles and standards set out within this document is consistent with the overarching information sharing principles agreement used across the Avon, Gloucester and Wiltshire area since 2003

2.0 Parties to this Agreement

2.1 All partners of the B&NES LSAB as listed in its Terms of Reference are party to this agreement.

3.0 Purpose of this Agreement

3.1 The purpose of sharing information between the designated organisations is to:

i. Ensure that relevant information about the alleged abuse of an adult at risk is shared between organisations and reported as an Alert to the relevant organisation i.e. Sirona Care and Health or AWP

ii. Enable a detailed investigation to take place

iii. Enable evidence to be considered in reaching a decision as to whether the abuse of an adult at risk has taken place

iv. Enable a multi-agency response to safeguard adults at risk from further abuse

NB: By sharing information, organisations will be able to identify adults at risk who are considered to be at risk of abuse. It is anticipated that nominated representatives from the organisations who are party to this agreement will be engaging in regular multi-agency case discussion in order to secure services for adults at risk and their carers.

4.0 Principles Governing the Sharing of Information

4.1 A number of safeguards are necessary to ensure a balance between maintaining confidentiality and sharing information appropriately. The key principles governing the sharing of information are detailed in the Data Protection Act 1998 and the Caldicott Report 2013. The Human Rights Act 1998, the Mental Capacity Act 2005 and the common law 'duty of confidentiality' are also relevant in this context (see Appendix 1).

4.2 The parties to this agreement are committed to ensuring that information is shared appropriately between those professionals working with adults at risk across Bath & North East Somerset and who have a legitimate need for that information to assist with investigating alleged abuse and delivering high quality, integrated services that meet assessed need.

4.3 All partner organisations will commit to the following principles in sharing information about adults at risk: -

a) The majority of personal information provided by individuals is confidential in nature. All partner organisations therefore accept that this information will not be disclosed without the consent of the individual concerned, unless there are statutory grounds to do so.

b) When seeking personal information from other parties to this Agreement, staff will respect the duty of confidentiality and will not seek to override the procedures which each organisation has in place to ensure personal information is not disclosed illegally or inappropriately.

c) All partner organisations accept that personal information processed under this agreement is only to be used for a specified purpose(s). The secondary use of personal information is not permitted unless the consent of the disclosing party to that secondary use is sought and granted, and/or regard is had to the provisions of this agreement.

d) Where it is appropriate, all partner organisations agree always to give consideration as to whether it is possible to use depersonalised information (namely information presented in such a way that individuals cannot be identified) to achieve the specified purpose.

e) All partner organisations agree to ensure that the personal information that may be accessible or shared is purposeful, justified and specifically geared to the task it is intended to serve. The information should be sufficient to serve the purpose, and any access and sharing of information should exclude unnecessary material.

f) All partner organisations agree that they will each comply with the specified statutory timescales relating to how long particular types of information are retained. Internal procedures will be put into place to ensure compliance with this obligation. Where there are no statutory guidelines, information will be held in accordance with the fourth and fifth principles of the Data Protection Act.

g) Subject to certain exemptions, all partner organisations are obliged to notify the Information Commissioner of all purposes for which they process personal data by automated means.

h) All partner organisations agree to ensure compliance with the notification requirements of the Data Protection Act and ensure that their notification is accurate and kept up to date.

i) All partner organisations agree to ensure that where it is appropriate, consent processes are in place which meet the requirements outlined within the Data Protection Act 1998.

j) All partner organisations agree to make every reasonable effort to ensure that the information they hold is accurate and up to date. Any errors identified in the information held will be corrected or erased as soon as reasonably practicable.

k) All partner organisations agree to make reasonable efforts to ensure that the recipients of personal information are kept informed of any changes to the personal information which they have received, so that records can be kept up to date.

l) All partner organisations will ensure efficient and effective procedures are put in place to address complaints relating to the processing of personal information.

m) All partner organisations will ensure that Subject Access Requests made to them are responded to in accordance with the requirements outlined within the Data Protection Act 1998.

n) All partner organisations agree that appropriate training will be given to staff so that they are aware of their responsibilities to ensure personal information is processed lawfully.

o) Should personal information be disclosed without legal justification, the partner organisation or organisations who committed the breach agree to ensure that a manager at the appropriate level of the organisation investigates the incident and considers ways in which the repetition of the error can be avoided in the future. The partner organisation who has committed the breach will notify the party who provided the information immediately and subsequently, the outcome of the investigation.

5.0 Adoption and Implementation of Principles

5.1 Partner organisations agree that the principles detailed in this agreement and its supporting practical guidance provide a secure framework for the sharing of information between their respective organisations, enabling compliance with their statutory and professional responsibilities.

5.2 The partner organisations agree to: -

a) Facilitate the sharing of information wherever such sharing is lawful and need can be demonstrated.

b) Implement this agreement within their organisation.

c) Disseminate to all staff who are directly involved in its implementation.

d) Ensure staff adhere to the procedures and arrangements set out in the protocol.

e) Provide evidence, when requested, that agreed procedures and arrangements have been implemented.

6.0 Monitoring and Review

6.1 The Agreement will be reviewed annually by the Policy and Procedures sub-group of the B&NES LSAB. Any required changes will be considered and brought to the attention of all partners of the B&NES LSAB.

7.0 Advice and Guidance

7.1 Further advice and guidance in relation to sharing information with regards vulnerable adults is available from B&NES Health and Wellbeing Partnership Commissioning arm.

Appendix 1

Safeguarding of Adults: Relevant Legislation relevant to sharing information

1.0 Introduction

1.1 The principles and supporting guidance set out within this agreement is consistent with the principles outlined within the overarching information sharing agreement that all partner organisations have adopted supporting guidance will help to explain more about such issues as to how, why and when to share information, when consent is needed and when consent is not required.

2.0 Confidentiality

2.1 Anything that applies to an individual and by which they can be identified, is personal information. For the purposes of this agreement "Confidential Information" means any information which has a necessary quality of confidence (however it is conveyed or on whatever media it is stored) including all personal data and sensitive personal data within the meaning of the Data Protection Act 1998.

2.2 A concern for confidentiality must not be used as a justification for withholding
information when it would be in the adult at risks best interest to share it.

2.3 The approach to information sharing with others must be the same whether practitioners are part of the same organisation or not. In practice there is likely to be implied consent for sharing information between practitioners in the same organisation, where this is justified.

2.4 Is the Information Confidential?

2.5 Some kinds of information, such as medical records and communications between doctor and patient, are generally recognised as being subject to a duty of confidence. Other information may not be, particularly if it is trivial or readily available from other sources or if the person to whom it relates would not have an interest in keeping it secret.

2.6 Maintaining Confidentiality

2.7 As a general rule you must treat all personal information you acquire or hold in the course of working with adults, children and families as confidential and take particular care with sensitive information.

2.8 Consent

2.9 There will be no breach of confidence if the person to whom a duty of confidence is owed consents to the disclosure. The person disclosing the

information has a duty to ensure that the person understood what was to be disclosed, to whom and for what purpose. A note should be made of the express or implied consent given.

2.10 Whose consent is required? The duty of confidence is owed to the person who has provided information on the understanding it is to be kept confidential and, in the case of medical or other records, the person to whom the information relates.

2.11 Has consent been given? You do not need express consent if you have reasonable grounds to believe that the person to whom the duty is owed understands and accepts that the information will be disclosed. For example, a person who refers an allegation of abuse to a social worker would expect that information to be shared on a 'need to know' basis with those responsible for following up the allegation. Anyone who receives information, knowing it is confidential, is also subject to a duty of confidence. Whenever you give or receive information in confidence you should ensure there is a clear understanding as to how it may be used or shared.

2.12 Should I seek consent? If you are in doubt as to whether a disclosure is authorised it is best to obtain express consent. But you should not do so if you think this would be contrary to a person's welfare. For example, if the information is needed urgently the delay in obtaining consent may not be justified. Seeking consent may prejudice a police investigation or may increase the risk of harm.

2.13 What if consent is refused? You will need to decide whether the circumstances justify the disclosure, taking into account what is being disclosed, for what purposes and to whom.

2.14 Sharing Information without Consent

2.15 There are exceptions in the Data Protection Act 1998 that permit disclosure of confidential information without consent or a court order.

2.16 The key factor in deciding whether or not to disclose confidential information is proportionality: is the proposed disclosure a proportionate response to the need to protect the individual. The amount of confidential information disclosed, and the number of people to whom it is disclosed, should be no more than is strictly necessary to meet the public interest in protecting health and well-being.

2.17 The more sensitive the information is, the greater the need must be to justify disclosure and the greater the need to ensure that only those professionals who have to be informed receive the material ('the need to know basis').

2.18 Is there a difference between disclosing information within your own organisation or between organisations? The approach to confidential information should be the same whether any proposed disclosure is internally

within one organisation e.g. within a hospital, or within social services or between agencies e.g. from a doctor to a social worker.

2.19 The need to disclose confidential information to others within your own organisation will probably arise more frequently than will be the case for inter-agency disclosure. For example a nurse will need to discuss confidential information with a doctor more frequently than with a social worker. It would probably be accepted that such discussions need to take place within the hospital, so there would usually be implied consent. But if not i.e. if you disclose information that someone has asked you to keep secret you will have to decide whether the circumstances justify the disclosure.

3.0 What are the Legal Restrictions?

3.1 The decision whether to disclose information may arise in various contexts. You may have a concern about someone that might be allayed or confirmed if shared with another agency. In all cases the main restrictions on disclosure of information are: common law duty of confidence; Human Rights Act 1998; and the Data Protection Act 1998.

3.2 Each of these has to be considered separately. Other statutory provisions may also be relevant, but in general the law will **not** prevent you from sharing information with other practitioners if: those likely to be affected consent; or the public interest in safeguarding the person's welfare overrides the need to keep the information confidential; or disclosure is required under a court order or other legal obligation.

3.3 The Data Protection Act 1998

3.4 The key legislation governing the obtaining, protection and use of identifiable personal data is the Data Protection Act 1998 (DPA). The DPA sets out a number of key definitions, including: -

a) **Personal Data:** This is defined as data which relates to a living individual, who can be identified from that data or from that data and other information in the possession of, or likely to come in to the possession of the Data Controller.

b) **Processing:** This is defined as any operation carried out on the personal data, including collecting, storing, using and disclosing that data.

c) **Data Controller:** This is defined as a person, who either alone or jointly with other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed.

d) **Data Subject:** This is defined as a living individual to whom personal data relates.

e) **Sensitive Personal Data:** This is defined as data within one of the following categories:
    - The racial or ethnic origin of the individual
    - Their political opinions
    - Their religious beliefs or beliefs of a similar nature
    - Whether they are a member of a trade union
    - Their physical or mental health or condition
    - Their sexual life
    - The commission or alleged commission by them of any offence
    - Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any Court in such proceedings

3.5 The DPA sets out eight principles that must be complied with when processing personal data. These principles are summarised below. The processing of personal information by the organisations party to this agreement must comply with these principles.

- Personal data must be processed fairly and lawfully
- Personal data must be processed for lawful and specified purposes
- Personal data held shall be adequate, relevant and not excessive in relation to the purposes for which it is processed
- Personal data must be accurate and where necessary, kept up to date
- Personal data must be held for no longer than is necessary
- Personal data shall be processed in accordance with the rights of data subjects under the Act
- Appropriate measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.
- Personal data shall 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 regarding the processing of personal data.

3.6 When sharing personal information, compliance with the first DPA principle is crucial to ensuring the sharing of the information is carried out lawfully.

3.7 To ensure that personal information is processed in a lawful manner, one of several specified conditions (set out in Schedule 2 of the Data Protection Act) must be complied with. These conditions are: -

- The individual has given his/her consent to the processing

- The disclosure is necessary to comply with a legal obligation

- The disclosure is necessary for the exercise of a statutory function, the administration of justice, or other public functions exercised in the public interest (e.g. for the purposes of a S17 assessment or S47 enquiry)

- The disclosure is necessary in order to protect the vital interests of the individual (this is envisaged to be a life and death scenario)

- The processing is necessary in order to pursue the legitimate interests of the organisation or certain third parties (unless prejudicial to the interests of the individual)

- The processing is necessary for the entering into a contract at the request of the individual or performance of a contract to which the individual is a party.

3.8 As a general rule, if one of the above conditions is satisfied, the processing of information is lawful. However, if the information to be processed is sensitive personal data, then one of the following conditions, which are contained in Schedule 3 of the DPA, must also be satisfied (as well as the conditions in Schedule 2 above) before processing that information:

- The individual has given their explicit consent to the processing of the personal information.

- The processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment.

- The processing is necessary to protect the vital interests of the individual or another person. Where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonably withheld where it is necessary to protect the vital interests of another.

- The processing is carried out in the course of its legitimate activities by any not for profit organisation which exists for political, philosophical, religious or trade-union purposes. The processing must be carried out with appropriate safeguards, relate only to the body's members of regular contacts, and not involve disclosure to a third party without consent.

- The information contained in the personal information has been made public as a result of steps deliberately taken by the individual.

- The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice.
- The processing is necessary for the administration of justice or carrying out legal or public functions.

- The processing is necessary for medical purposes and is undertaken by a health professional or equivalent.

- The processing is of sensitive personal data relating to racial or ethnic origin, is necessary for the purposes of equal opportunity monitoring, and is carried out with appropriate safeguards in place.

3.9 If you are making a decision to disclose personal data you must comply with the Act, which includes the eight data protection principles. These should not be an obstacle if: -

- you have particular concerns about the welfare of an adult at risk;

- you disclose information to social services or to another professional; *and*

- the disclosure is justified under the common law duty of confidence.

3.10 Where personal information is given to professionals in confidence, then in addition, the common law duty of confidentiality must also be considered.

3.11 Individuals' Rights under the Data Protection Act 1998

3.12 The DPA gives seven rights to individuals in respect of their own personal data held by others. They are:-

a) Right of subject access

b) Right to prevent processing likely to cause damage or distress

c) Right to prevent processing for the purposes of direct marketing

d) Rights in relation to automated decision making

e) Right to take action for compensation if the individual suffers damage

f) Right to take action to rectify, block, erase or destroy inaccurate data

g) Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

3.13 Subject to certain exceptions, any living person who is the subject of information held and processed by an organisation has a right of access to that information.

3.13 Where access is refused, the individual may appeal.

3.14 There are certain statutory exemptions that may limit access rights. These include for example where personal information is subject to legal professional privilege.

3.15 The Common Law Duty of Confidentiality

3.16 The circumstances in which a common law duty of confidence arises have been built up in case law over time. The duty arises when a person shares information with another in circumstances where it is reasonable to expect that the information will be kept confidential. The courts have found a duty of confidence to exist where: -

- The information has a necessary quality of confidence

- The circumstances of the disclosure have imposed an obligation on the confidant to respect the confidence. This usually means considering whether the information was imparted for a limited purpose.

3.17 Most of the personal information processed by the partner organisations under this Agreement will be of a confidential nature. Therefore, as a general rule, this confidential information should not be disclosed without the consent of the data subject. However, the law permits the disclosure of confidential information where there is an overriding public interest or justification for doing so.

3.18 The Human Rights Act 1998

3.19 Article 8(1) provides that: -

> "Everyone has the right to respect for his private and family life, his home and his correspondence"

3.20 However, this is a qualified right and Article 8 (2) states that: -

> ''There should be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic wellbeing 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 freedoms of others''.

3.21 Therefore, disclosure of personal information must take Article 8 into consideration. The sharing of personal information may be necessary, for example, for the protection of health or morals, for the prevention of the rights and freedoms of others or for the prevention of disorder or crime.

3.22 Caldicott Guardian

3.23 Although not a statutory requirement, partner organisations are committed to the Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared. These are:-

Caldicott Principles (Revised September 2013)
Principle One: Justify the Purpose Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate Guardian.
Principle Two: Don't use personal data unless it is absolutely necessary Personal identifiable information data should not be included unless it is essential for the specified purpose(s) of that flow. The need for services users to be identified should be considered at each stage of satisfying that purpose.
Principle Three: Use the minimum necessary personal confidential data Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.
Principle Four: Access to personal confidential data should be on a strict need to know basis Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
Principle Five: Everyone with access to personal confidential data should be aware of their responsibilities Action should be taken to ensure that those handling personal confidential

Data - both clinical and non-clinical staff - are made fully aware of their individual responsibilities and obligations in to respect patient confidentiality.
Principle Six: Comply with the law Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements
Principle Seven: The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

3.24 The Mental Capacity Act 2005

3.25 This Act was introduced to provide a clearer legal basis for making decisions and in doing so, promotes best practice in supporting anyone who is unable to make some or all decisions for themselves. The inability to make a decision could be because of a learning disability, mental health problems, brain injury, dementia, alcohol or drug misuse, side effects of medical treatment or any other illness or disability.

This Act sets out in detail how capacity to make decisions should be assessed. The principles of the Act should be followed in the event that a person needs to be asked for specific consent to his information being used or shared for a particular purpose. In particular, it should be assumed that a person does have the capacity to consent to the processing of his information, unless this is proved otherwise taking into account all the relevant circumstances at the relevant time.

Chapter 16 of the Mental Capacity Act Code of Practice[1] offers guidance on: -

- What personal information about someone who lacks capacity people
  involved in their care have the right to see; and

- how they can get hold of that information.

PRACTICE NOTE
Questions to consider when requesting personal information about someone who may lack capacity
• Does the adult at risk have capacity to agree that information can be

disclosed? Have they previously agreed to disclose the information?

- What information do I need?
- Why do I need it?
- Who has the information?
- Can I show that: -
  - I need the information to make a decision that is in the best interests of the person I am acting for; and
  - the person does not have the capacity to act for themselves?
- Am I acting under a Lasting Power of Attorney or as a Deputy with specific authority?
- Do I need to share the information with anyone else to make a decision that is in the best interests of the adult at risk who lacks capacity?
- Should I keep a record of my decision or action?
- How long should I keep the information for?
- Do I have the right to request the information under section 7 of the Data Protection Act 1998?
- Is the request covered by section 7 of the Data Protection Act 1998? Is the request being made by a formally authorised representative?
  - If not:
    - Is the disclosure legal?
    - Is the disclosure justified, having balanced the person's best interests and the public interest against the person's right to privacy?

PRACTICE NOTE

Questions to consider in deciding whether disclosing the information to an individual or organisation who have requested it is legal or justified

- Do I (or does my organisation) have the information?
- Am I satisfied that the adult at risk lacks capacity to agree to disclosure?
- Does the individual or organisation person requesting the information have any formal authority to act on behalf of the person who lacks capacity?
- Am I satisfied that the individual or organisation making the request: -
  - Is acting in the best interests of the adult at risk?
  - Needs the information to act properly?
  - Will respect confidentiality?
  - Will keep the information for no longer than necessary?
- Should I get written confirmation of these things?

A person may have the capacity to agree to someone seeing their personal information, even if they do not have the capacity to make other decisions. In some situations, a person may have previously given consent (while they still had capacity) for someone to see their personal information in the future.

Healthcare and social care staff may disclose information about somebody who lacks capacity only when it is in the best interests of the person concerned to do so, or when there is some other lawful reason for them to do so.

For disclosure to be in the public interest, it must be proportionate and limited to the relevant details. Healthcare or social care staff faced with this decision should seek advice from their legal advisers. It is not just things for 'the public's benefit' that are in the public interest – disclosure for the benefit of the person who lacks capacity can also be in the public interest (for example, to stop a person who lacks capacity suffering physical or mental harm).

3.6 Other Statutory Provisions

Section 115 of the Crime and Disorder Act 1998 enables any person to disclose information to a relevant authority for any purposes of the Act if they would not otherwise have the power to do so. Relevant authorities include local authorities, NHS bodies and police authorities. The purposes of the Act broadly cover the prevention and reduction of crime and the identification or apprehension of offenders.

Appendix 2

Practical Guidance – Questions to ask if you want to share information about an adult at risk

Practitioners must make sure that they follow these guidelines when sharing information within their own organisations as well as when sharing information with other agencies.

These questions are to help practitioners build up their confidence in information sharing, not to find reasons for not sharing information.

Why do I/they want this information?
• The purpose of the information sharing should be explicit • The information sharing may be justified if the purpose of the sharing is clearly in the best interests of the adult at risk
PRACTICE GUIDANCE
Practitioners must be clear regarding the purpose of the request for information. This can be expressed in general terms, but needs to relate to the welfare of the adult at risk. This may call for some thought and judgment, but must not be used as a barrier to information sharing.

Can I/they demonstrate sufficient need to know?
• The actions taken or services given should be different after the information is known • The information is necessary for the performance of a job or a statutory function
PRACTICE GUIDANCE
As indicated above, practitioners must be clear about why they are seeking information from any specific source. Consideration must be given as to the difference that knowing the new information will make. The more explicit a practitioner can be, the easier it is to know if the information sharing is appropriate.

Is the request proportionate to the purpose for which the disclosure is sought?

- The information shared must be the minimum necessary to achieve the aim

PRACTICE GUIDANCE

We frequently like to know the 'whole story'. However, it is not usually necessary. Even within an organisation, practitioners must limit what they share. If the purpose is clear, then what information is necessary to achieve that purpose will also become clearer.

Is the information up to date and accurate?

- Many difficulties with information sharing arise because the information is not accurate or because an opinion is given as fact

PRACTICE GUIDANCE

Many organisations have good routines for checking data. It is often worth checking factual information with the adult at risk before it is shared. This can be done by letting the adult at risk or their representatives see a copy of the report before it is sent. Practitioners must be careful to acknowledge opinions and judgements, including the source.

Will the request involve secondary disclosure?

- Information belongs to the person or agency that supplies it
- Information must not be passed to a third party without consent
- Information gathered for one purpose cannot be used or passed on for a different purpose

PRACTICE GUIDANCE

When considering the sharing of information supplied by another professional or agency, it is important to check whether you have consent to do so.

It is also important to check that the information is accurate and still valid.

It is advisable that, wherever possible, the person or organisation who 'owns' and supplied the information is asked for their consent to share that information, at the same time checking its accuracy.

Do I need consent?

- In most cases there is a legal requirement to obtain consent before any personal information can be shared
- Consent can be implied
- Failure to gain consent may make the individual practitioner and the agency liable to prosecution
- The adult at risk must understand what they are agreeing to and the practitioner must record that consent has been given
- If the adult at risk appears to lacks capacity to consent then the process for assessing mental capacity must be followed

PRACTICE GUIDANCE

Consent can be implied. This means that what someone does implies that they agree for information to be shared. For example, if you agree to see a nurse for a test it is assumed that you have given your consent for the results to be shared with your doctor and certain other specific professionals concerned with your care.

Most services assume consent to share certain information with colleagues within the organisation. It is good practice to make this as clear as possible to all parties through the information given out at the first contact. Leaflets and posters can remind all parties about what information is held and how it is used.

A practitioner should discuss information sharing at the first contact or first available opportunity with the adult at risk or their representative. If the person is appears to lack capacity to consent then the process for assessing mental capacity must be followed.

Additional detail relating specifically to consent is detailed in Section 3.5 above.

Have I got consent?

- Consent must not be assumed
- Practitioners must check whether the adult at risk still gives consent, particularly if circumstances change
- Practitioners must know what to do if consent is refused (further details within the next section of this Guidance)

PRACTICE GUIDANCE

Consent can be given verbally. However, this must be recorded, clearly timed and dated. In this case practitioners must also note the outcome of discussions about any restrictions that the individual has placed on the type of information that can be shared, or the organisations with whom it can be

shared.

If an agency uses a Consent Form, it must be stored in the adult at risk's file. A copy of the Consent Form must be given to the adult at risk.

If the adult at risk has placed a limit on the disclosure of information in any way, then this needs to be clearly indicated.

Consent to disclosure of personal information must not be viewed as lasting 'forever'. An adult at risk may decide to withdraw consent previously given. In any event consent must be limited for an appropriate period. A record should be kept of the date on which consent was given and if it is subsequently withdrawn the date on which this occurs must be recorded. If consent has not been requested or has not been revisited for a significant period of time, then it should be sought.

If a professional receives a request to share personal information they should check the appropriate file to see whether there is a current or valid consent, either as a Form or an appropriate record and whether any restrictions have been placed on consent.

When information is sought a professional who is already working with an individual may well have a valid consent covering that specific request. In this case you must seek a copy.

If I cannot get consent is there another justification for disclosure?

Failure to share information appropriately can:

- Increase the risk to the adult at risk
- Result in a failure to provide adequate care and services
- Prevent appropriate decisions being made

Sharing information without consent may be necessary and appropriate under some circumstances such as: -

- When an adult at risk is believed to be at serious risk of harm
- When there is evidence of serious public harm or risk of harm to others
- Where there is evidence of serious health risk to an adult at risk
- For the prevention, detection or prosecution of serious crime
- When instructed to do so by a Court

PRACTICE GUIDANCE

This is a difficult and complex area. In practice, a decision to share without

consent may most often be made in cases concerned with Safeguarding Adults.

Decisions to share personal or sensitive information without consent must only be taken by staff with an appropriate level of knowledge and authority. Staff taking on this role must be provided with clear guidance to enable them to decide whether there are statutory grounds for disclosure without consent. They must also have access to appropriate legal advice should this be necessary. Within Safeguarding Adults such a member of staff will be at Safeguarding Adults Lead Worker level or above.

Agencies need to have arrangements in place to be able to authorise such disclosures in emergencies.

Where information is shared without consent, details about the information shared, the reasons why the decision to share the information was taken, the person who gave the authorisation to share the information and the person with whom the information was shared must all be recorded.

Recipients of information that has been disclosed without consent must be made aware of this as well as the basis on which the decision to disclose has been made.

The recipient should put agreed security procedures in place.

It is good practice for the adult at risk to be informed that information has been shared without consent. However, there may be circumstances where this is not possible or where caution needs to be exercised around the timing of such action, particularly within more complex safeguarding situations.

Have I recorded that I have shared this information?

- Practitioners must keep a dated record of what information has been shared and with whom it has been shared

PRACTICE GUIDANCE

It is not necessary to keep separate records regarding the sharing of information. However, any case log, case record or event sheet must include a note of any such requests and ensuing conversations concerning sharing information.

Reports and other written communications must be filed with a note recording to whom they were sent with reference made to the sharing of such Information within case records as deemed appropriate.

Am I sharing this information in a secure way?

'Secure' means that all reasonable steps have been taken to prevent the information being passed to someone that does not have the right to it.

PRACTICE GUIDANCE

Information must always be shared in a way that is consistent with your own agency or organisation's policy and procedures. Responsibility for the security of information being shared lies with the 'sender' of that information.

Sharing Verbally: If information is to be shared over the phone, steps need to be taken to ensure that the recipient is properly identified. Your organisation's policy may require you to take and check a number and telephone the recipient back. If information is to be left on a voicemail or answer machine, check that the intended recipient is the only person who has access to that device.

Sharing by Post: Consideration should be given to such matters as the arrangement used by the recipient for the opening of post, the labelling of an envelope containing confidential information and so on. It would also be useful to consider your own agency's practice for the receipt of confidential post.

Sharing by E-mail and text: E-mail and texts are not an especially secure way to share information. Prior to sharing information in this way the sender needs to establish the security level of the sending and recipient servers. Wherever possible a secure internet gateway, such as PSN, should be used. In addition, if sending an e-mail to a recipient for the first time, a careful check should be made that the e-mail address is correct.

Sharing by fax: As with sharing by phone, you may wish to ensure that you have the correct number and know the recipient. You may also wish to ensure that the fax is collected on receipt rather than being left on the machine for anyone to pick up and read. Your own agency's policy and procedures should help clarify such matters.