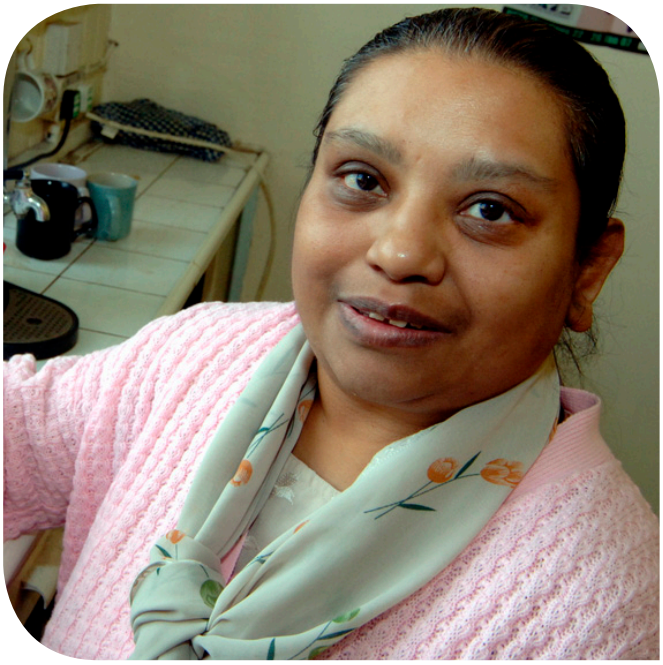
social care
institute for excellence

ADULTS SERVICES WEB RESOURCE

Protecting adults at risk: Good practice guide



Information sharing

This section is intended to help managers and practitioners make appropriate decisions concerning the sharing of information when acting to investigate and prevent significant harm occurring to adults at risk.

Each London borough will have its own local agreement on how it shares information with other agencies in the area, and this normally consists of a signed document or policy setting out a framework and process.

This guidance is intended to underpin and reinforce local arrangements and adheres to government guidelines on the sharing of information.

Introduction

There is a recognition among partner agencies of the value of working together as a means of protecting the public, and the importance of information sharing as a means to achieve excellent partnerships. Agencies should seek to share information with partners where there is a lawful reason to do so and when there is an opportunity to make a positive impact on public protection, in keeping with the key safeguarding principle of partnership.

The most recent discussion of all aspects of patient-identifiable information and how this is to be protected is to be found in the Caldicott Committee Report on the review of patient-identifiable information (**3**) The report recognises that confidential patient information may need to be disclosed in the best interests of the patient, and discusses in what circumstances this may be appropriate and what safeguards need to be observed.

The principles can be summarised as:

- information will only be shared on a ‘need to know’ basis
- confidentiality must not be confused with secrecy
- informed consent should be obtained but, if this is not possible and other vulnerable adults are at risk, it may be necessary to override the requirement
- it is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations where other vulnerable people may be at risk.

Decisions about who needs to know and what needs to be known should be taken on a case-by-case basis, in line with agency policies and the constraints of the legal framework.

Principles of confidentiality designed to safeguard and promote the interests of service users and patients should not be confused with those designed to protect the management interests of an organisation. These have a legitimate role but must never be allowed to conflict with the interests of service users. If it appears to an employee or person in a similar role that such confidentiality rules may be operating against the interests of vulnerable adults, then a duty arises to make full disclosure in the public interest (**4**).

A summary of the legal framework

The main legal framework relating to the protection of personal information is set out in:

- the Human Rights Act 1998, which incorporates Article 8 of the European Convention on Human Rights (ECHR), including the right to a private and family life
- the common law duty of confidentiality
- the Data Protection Act 1998, covering protection of personal information.

Here we summarise these pieces of legislation and others; however, legal advice needs to be sought for a more detailed interpretation of the main requirements of each.

There is no general statutory power to share information, just as there is no general power to obtain, hold or process data. Some Acts of Parliament give public bodies express statutory powers to share information. These are often referred to as 'statutory gateways' and provide for the sharing of information for particular purposes. These gateways may be permissive or mandatory.

- An example of a 'permissive statutory gateway' is Section 115 of the Crime and Disorder Act 1998, which permits people to share information to help prevent or detect crime.
- An example of a 'mandatory statutory gateway' is Section 8 of the National Audit Act 1983, which imposes a legal obligation on public bodies to provide relevant information to the National Audit Office.

Where there is no express statutory power to share information it may still be possible to imply such a power from the other duties and powers public bodies have. Many activities of statutory bodies will be carried out as a result of implied statutory powers, particularly as it may be difficult to expressly define all the numerous activities that a public body may carry out in the process of delivering its main duties and exercising its powers.

Having express or implied statutory powers in any particular case does not mean that the Human Rights Act 1998, the common law duty of confidentiality and the Data Protection Act 1998 can be disregarded. Where a statutory gateway explicitly removes the need to consider confidentiality, then confidential information can be shared; however, this will be rare and will apply in limited circumstances. Where there are implied powers you need to consider the language of the gateway and the surrounding circumstances.

The Human Rights Act 1998

The ECHR confers a positive obligation on public authorities to take reasonable steps within their powers to safeguard the rights of individuals. Article 8 of the ECHR was incorporated into UK law by the Human Rights Act 1998 and recognises a right to respect for private and family life.

- Article 8.1: everyone has the right to respect for his private and family life, his home and his correspondence.

> Article 8.2: there shall be no interference by a public authority with exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of crime or disorder, protection of health and morals or for the protection of rights and freedoms of others.

Sharing confidential information may be a breach of an individual's Article 8 right; the question is whether sharing information would be justified under Article 8.2, and whether it would be proportionate. You need to consider the pressing social need, whether sharing the information is a proportionate response to this need, and whether these considerations can override the individual's right to privacy. If an adult is at risk of serious harm, or sharing information is necessary to prevent crime or disorder, interference with the individual's right may be justified under Article 8.

The common law duty of confidentiality

The common law duty of confidentiality provides that where there is a confidential relationship, the person receiving the confidential information is under a duty not to pass on that information to a third party. However, this duty is not absolute and information can be shared without breaching the common law duty if:

- the information is not confidential in nature
- the person to whom the duty is owed has given explicit consent
- there is an overriding public interest in disclosure
- sharing is required by a court order or other legal obligation.

The Data Protection Act 1998

The Data Protection Act 1998 deals with the processing of personal data (both sensitive and non-sensitive). Personal data is data which relates to a living person, including the expression of any opinion or indication of intentions in respect of the individual concerned. Sensitive personal data is that relating to racial or ethnic origin, religious or other similar beliefs, physical or mental health condition, sexual life, political opinions, membership of a trade union, the commission or alleged commission of any offence, any proceedings for an offence committed or alleged to have been committed, the disposal of proceedings or the sentence of any court in proceedings.

Information about an individual will often contain data from several sources – for example, from care agencies, doctors or the police – and may contain their name and address. Such information may also include data about other people – for example, the individual's family members. These people are usually referred to in the Data Protection Act as 'third parties'. Information about third parties is personal information and should be treated accordingly.

If an individual is no longer alive their personal information is not covered by the Data Protection Act, although a duty of confidence may require some or all of their personal information to be kept confidential.

Organisations which process personal data must comply with the data protection principles set out in Schedule 1 of the Data Protection Act. These require data to be:

- fairly and lawfully processed: in particular, data shall not be processed unless a Schedule 2 condition is met, and if sensitive personal data, a Schedule 3 condition
- processed for limited specified purposes
- adequate, relevant and not excessive for those purposes
- accurate and up to date
- kept for no longer than necessary
- processed in accordance with the data subject's rights under the Data Protection Act
- kept secure
- not transferred to non-European economic areas (EEAs) without adequate protection

Personal data must not be processed unless at least one of the conditions in Schedule 2 of the Data Protection Act ('the conditions for processing') is met and, in the case of processing sensitive personal data, at least one of the conditions in Schedule 3 ('the conditions for processing sensitive data'). However, meeting a Schedule 2 and a Schedule 3 condition will not, on its own, guarantee that processing is fair and lawful. The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.

Schedule 2 conditions include:

- the data subject has given consent to the data processing
- the processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject with a view to entering into a contract
- the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract
- the processing is necessary to protect the data subject's vital interests
- the processing is necessary for the administration of justice; for the exercise of any functions of either House of Parliament; for the exercise of any functions conferred on any person by or under any enactment; or for the exercise of any functions of the Crown, a minister or a government department; or for the exercise of any other public functions in the public interest by any person
- the processing is necessary for the purposes of the legitimate interests of the data controller, or of the third party or parties to whom the data is disclosed, except where the processing is unwarranted by reason of the rights, freedoms or interests of the data subject.

When information is sensitive then a Schedule 3 condition must also be met. These are:

- the data subject has given explicit consent to the processing

- the processing is necessary for the purposes of exercising any legal right or obligation on the data controller in connection with employment
- the processing is necessary to protect the vital interests of the data subject or someone else, in a case where the data subject cannot give consent or consent cannot reasonably be obtained, or, in order to protect another person's vital interests, the data subject is unreasonably withholding consent
- the processing is carried out by a not-for-profit body in the course of its legitimate activities and does not involve disclosure of the personal data to a third party without consent
- the information has been made public as a result of steps taken by the data subject
- the processing is necessary for the purposes of, or in connection with, any legal proceedings, obtaining legal advice or to establish, exercise or defend legal rights
- the processing is necessary for the administration of justice; for the exercise of any functions of either House of Parliament; for the exercise of any functions conferred on any person by or under any enactment; or for the exercise of any functions of the Crown, a minister or a government department
- the processing is necessary for medical purposes and is undertaken by a health professional
- the processing is of sensitive personal data consisting of information as to racial or ethnic origin, is necessary for the purpose of promoting racial or ethnic equality and is carried out with appropriate safeguards.

There is other 'gateway' legislation where cooperation between statutory bodies includes the sharing of information. Below are the Acts most relevant to safeguarding adults at risk.

The Criminal Justice Act 2003

The Criminal Justice Act sets out the arrangements for assessing the risk posed by different offenders. These include relevant sexual and violent offenders and other persons who are considered by the responsible body to be a serious risk to the public. The responsible bodies in this case are the police, probation and prison services. There is a duty on social services to cooperate with these arrangements and that cooperation may include the exchange of information. The arrangements will be familiar to people as multi-agency public protection arrangements (MAPPA).

The Crime and Disorder Act 1998

The Crime and Disorder Act recognises that key authorities, such as councils and the police, have a responsibility for the delivery of a wide range of services within the community. Section 17 places a duty on them to do all they reasonably can to prevent crime and disorder in their area. Local partnerships will exist to address crime reduction. Section 115 provides any person with the power, but not an obligation, to disclose information to responsible public bodies (e.g. the police, health

or local authorities) and their cooperating bodies in pursuing a local crime and disorder strategy. Therefore, this can cover circumstances of criminal activity, but also civil law proceedings and local initiatives of crime prevention and reduction.

The Immigration and Asylum Act 1999

Section 20 of the Immigration and Asylum Act provides for a range of information sharing to undertake the administration of immigration controls to detect or prevent criminal acts under this legislation.

The Mental Capacity Act 2005

There will be circumstances where an individual adult appears not to be able to make a decision about whether to consent to information being shared with others.

The Mental Capacity Act and the associated code of practice contain guidance about the consideration of a person's capacity, or lack of capacity, to give consent to sharing information. The starting assumption must be that the person has capacity unless it is established that they do not, and only then after all practical steps to help the person make the relevant decision have been taken but have been unsuccessful. An unwise decision taken by the relevant person does not mean they lack capacity. Where a decision is made on behalf of the person who lacks capacity to share personal information it must still comply with the requirements of the Data Protection Act and be in their best interests.

Sharing health information can be a contentious area. There is guidance from professional health bodies, which NHS staff refer to, as well as local health trust policies. Local practice agreements need to be in place to ensure consistency across health and social care agencies and it is advisable to find out what these arrangements are when seeking the cooperation of health care staff. The most relevant piece of legislation is outlined briefly below.

The National Health Service Act 2006

Section 82 of the National Health Service Act 2006 places a duty on the NHS and local authorities to cooperate with one another in order to secure and advance the health and welfare of people, which would indicate the requirement to share information.

Practical steps to ensure consent and appropriate information sharing

The No secrets guidance (**4**) on which local safeguarding adults policies were developed prior to the adoption of the pan-London multi-agency policies and procedures, emphasised the need for joint working to safeguard adults. The guidance recognised a need to balance confidentiality with the need to protect adults at risk, and through the establishment of multi-agency safeguarding committees or boards, laid down a strong expectation of collaborative working. In May 2011, the government gave a clear indication that safeguarding adults boards would be placed on a statutory footing in 2012, requiring the cooperation of partners.

Obtaining consent to share information

If collaborative, multi-agency working is the normal response to safeguarding concerns, then the adult at risk or other person who is the focus of the safeguarding referral needs to be made aware at the earliest opportunity of the need to share

information, and to give their consent, if able to do so. This should where possible take the form of something explicit such as signing part of an assessment form with an appropriate information-sharing paragraph inserted; signing a separate consent form; or the referring professional or investigating officer making a clear record. Whatever the practice locally, consent to sharing information should be part of the explanation process to a person early in their contact with any professional who becomes aware of a safeguarding concern.

Where it is not possible for the person to consent to sharing information, after full consideration of the Mental Capacity Act code of practice, a best-interests decision will need to be made. Involved family or friends must be consulted on this decision but they cannot 'sign for' the person without capacity unless they have been authorised to act as a deputy for that person by the Court of Protection, or they have LPA for the person's health and welfare from the OPG. Routine sharing of information would not require a full decision-making process to demonstrate 'best interests' and guidance is available in the relevant code of practice on levels of decision-making for a person without capacity. However, any professional involved should be able to point to evidence of the need for protection in order to demonstrate that information is being shared appropriately.

Refusal to consent to share information

It is not possible to cover here all the circumstances where a person may withhold consent to share information. A common example is where the alleged victim of financial abuse withholds consent to share information with the police out of loyalty to a family member, who is the perpetrator. In these circumstances the professional receiving the information or investigating the abuse can inform the police if they believe a crime has been committed under the Crime and Disorder Act 1998. However, securing the cooperation of the alleged victim to pursue a prosecution in these circumstances is unlikely to be successful.

If consent is not obtained to share information in a safeguarding matter, there are several considerations to be made about sharing information without consent. Sharing information without consent can be legitimate where there is an overriding public interest, such as where sharing it could help in detecting crime, apprehending offenders, maintaining public safety, and the administration of justice. An example might be an abuser targeting older people in a particular locality where the victims do not want to take action, but others might also be at risk.

There is also the notion of 'legitimate purpose' in sharing information without consent, which can include issues such as:

- preventing serious harm to an adult at risk – including through prevention, detection and prosecution of serious crime
- providing urgent medical treatment
- implementing the Department of Health's 'No Secrets' agenda of protecting adults at risk from abuse

Information can also be shared without consent where the 'vital interests' of the individual are affected (and he or she cannot give consent or consent cannot reasonably be obtained); or where there is a legal duty.

Holding and sharing information: meetings

All agencies involved in safeguarding adults at risk operate within the Data Protection Act and should comply with that Act's requirements on the handling, recording and storing of sensitive information. In relation to safeguarding adults at risk, there are key documents involved in the process (e.g. investigation report and safeguarding conference notes) that need special consideration given their often very confidential contents. Where safeguarding meetings are held it is good practice to have a statement on confidentiality included in the agenda for the meeting and/or read out by the chair of the meeting. Particular consideration should be given to people attending who may not be accustomed to the requirements of confidentiality. An example of a simple statement is set out below:

This meeting is held under the London multi-agency policy and procedures to safeguard adults at risk. All matters presented are confidential to the individuals attending and the agencies they represent. The record of the meeting is distributed on the strict understanding that it will be kept confidential and stored securely. In some circumstances it may be necessary to make the record of this meeting available to other agencies not directly involved (e.g. the civil and criminal courts). Attendees and the agencies they represent should seek the advice of the chair of the meeting if they wish to share the record with others.

Inter-borough and general sharing of information

The Association of Directors of Adult Social Services (ADASS) has set out safeguarding standards which include the following guidance (please note that Protection of Vulnerable Adults (POVA) and Proceeds of Crime Act (POCA) lists have been superseded by ISA referrals):

The wishes of an adult with mental capacity should normally be respected. However, statutory agencies must act to uphold the human rights of all citizens and where others are at risk this duty will take precedence. Any action taken by an organisation to safeguard an adult should meet human rights standards. It should be proportionate to the perceived level of risk and seriousness. Intervention should not be arbitrary or unfair. It must have a basis in law: e.g. acting with the consent of the adult or, under duty of care, acting in the best interest of the adult; undertaken to secure a legitimate aim (e.g. to prevent a crime or protect the public); and be necessary to fulfil a pressing social need.

Raising concerns about abuse or neglect nearly always involves sharing information about an individual that is both personal and sensitive (Data Protection Act 1998). Such information about an adult with mental capacity should be shared only with their informed consent, unless there is an overriding duty such as a danger to life or limb, or risk to others. These exceptions are described in the Data Protection Act (1998) and 'Caldicott guidance' (DH 1997),[3] and case law in relation to human rights legislation. Information about an adult who may be at risk of abuse or neglect must be shared only within the framework of an appropriate information-sharing protocol. Information about a potential perpetrator of abuse must also be shared under an appropriate information-sharing protocol. Local provisions such as MAPPA meetings and national provisions such as the POVA and POCA lists should be used. (5)