



4LSAB Multi-Agency Guidance on Information Sharing

June 2024

Contents	Page
1. Guidance on Information Sharing – Introduction	3
2. Who is this guidance for?	3
3. Key principles of information sharing	4
4. Contexts for sharing information in adult safeguarding	5
5. Why do we need to share adult safeguarding information?	5
6. Sharing information to prevent abuse or neglect	6
7. Seven golden rules to sharing information	6
8. Legal basis for sharing information	7
8.1. Care Act 2014	7
8.2. Sharing information with the LSAB	7
8.3. Legislation giving powers or duties to share information	7
8.4. Decision-making about sharing information	8
8.5. What if a safeguarding partner is reluctant to share information?	9
8.6. What if an adult does not want their information shared?	10
8.7. Impact of sharing or withholding information	11
8.8. Managing allegations against people in a position of trust	11
8.9. Referring to the Disclosure and Barring Service	12
8.10. Professional codes of practice	12
8.11. Duty of Candor	12
8.12. Commissioning	13
8.13. Multi Agency Safeguarding Hubs	13
9. Confidentiality	13
10. Recording	14
10.1. Record Keeping	14
10.2. Meetings and Notes	15
10.3. Access to Records	15
11. The Caldicott Principles	16
12. Links to relevant information	16

1. Introduction - Guidance on Information Sharing

Sharing the right information, at the right time, with the right people, is fundamental to good practice in safeguarding adults. The Care Act 2014 emphasises the need to empower people, to balance choice and control for individuals against preventing harm and reducing risk, and to respond proportionately to safeguarding concerns. Information sharing is essential for effective safeguarding and promoting the welfare of adults with care and support needs. It is a key factor identified in many safeguarding adult reviews (SARs), where poor information sharing has resulted in missed opportunities to take action that keeps adults at risk safe.

The four Local Safeguarding Adults Boards covering Hampshire, Isle of Wight, Portsmouth and Southampton (4LSAB) have developed this guidance which is designed to support safeguarding partner organisations to understand their roles and responsibilities when seeking to co-operate with one another to share information for safeguarding purposes in accordance with the statutory guidance provided by the Care Act 2014 and the strengthened protections on personal data in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).

This guidance applies to sharing information about adults at risk. For guidance on information sharing about children, see the [HIPS Safeguarding Procedures Manual section on Information Sharing](#).

The 4LSABs acknowledge that partner agencies will already have in place information sharing agreements and/or protocols to enable and facilitate effective inter-agency communication, partnership working and decision making. This guidance builds on, rather than replaces these. Staff and volunteers must follow the relevant information sharing policies within their organisation which will address the key points from the [Information Commissioner's Office's Data Sharing Code of Practice](#) including:

- Identify your objective in sharing the data
- Be clear as to what data you are sharing
- Consider the benefits and risks of sharing and not sharing
- Ensure you follow the data protection principles
- Check your data sharing is fair and transparent
- Identify at least one lawful basis for sharing the data before you start sharing it
- Allow data subjects to exercise their individual rights easily
- Share data in an emergency as is necessary and proportionate. Plan ahead as far as possible
- Document your decisions about the data sharing, evidencing your compliance with data protection law.

2. Who is this guidance for?

This guidance is for all frontline practitioners and senior managers working with adults with care and support needs and carers who have to make decisions about sharing personal information for safeguarding purposes on a case-by-case basis.

3. Key principles of information sharing

The 4LSABs endorse the following principles to guide decision-making about sharing safeguarding information:

- The six statutory Safeguarding Principles must underpin all safeguarding practice, including information sharing.
- Adults have a general right to independence, choice and self-determination including control over information about themselves. In the context of adult safeguarding these rights can be overridden in certain circumstances.
- Relevant information can be shared with the relevant emergency services without consent to protect someone's life.
- The law does not prevent the sharing of sensitive, personal information **within** organisations. If the information is confidential, but there is a safeguarding concern, sharing it may be legally justified.
- The law does not prevent the sharing of sensitive, personal information **between** organisations where the public interest served outweighs the public interest served by protecting confidentiality – for example, where a serious crime may be prevented.
- Information can and should be shared lawfully within the parameters of the Data Protection Act 2018 and the UK GDPR.
- There should be local agreements or protocols in place setting out the processes and principles for sharing information between agencies.
- An individual employee cannot give a personal assurance of confidentiality.
- Frontline staff and volunteers should always report safeguarding concerns in line with their organisation's policy – this is usually to their line manager in the first instance except in emergency situations.
- It is good practice to try to gain the person's agreement to share information. As long as it does not increase risk, practitioners should inform the person if they need to share their information against the person's wishes.
- Practitioners should be aware of their respective organisation's escalation routes and whistleblowing policies and procedures.
- The management interests of an organisation should not override the need to share information to safeguard adults at risk of abuse.

4. In what contexts might safeguarding information need to be shared?

This guidance covers information sharing in a range of contexts to safeguard adults with care and support needs. It reflects relevant legislation the key principles agreed by the 4LSAB and is based on the best practice outlined in the [Social Care of Excellence \(SCIE\) Safeguarding Adults – Information Sharing](#) guidance:

Contexts in which information might need to be shared to safeguard adults with care and support needs:

- Raising concerns about abuse or neglect (or risk of this) of an adult with care and support needs.
- Undertaking safeguarding enquiries and sharing the outcomes.
- Responsibilities to share information and make referrals to the Disclosure and Barring Service (DBS) and/or professional bodies.
- Exchange information in the context of allegation management with the relevant Safeguarding Allegations Management Advisor (SAMA).
- Exchange information between the SAMA and the Local Authority Designated Officer (LADO) concerning children.
- Share information arising from the context of a Safeguarding Adults Review or other form of multi-agency learning review.

5. Why do we need to share adult safeguarding information?

Sharing safeguarding information with the right people at the right time is necessary in order to:

- Help people to access the right kind of support to promote and maintain wellbeing in order to prevent or delay the deterioration of need.
- Prevent abuse and harm that may increase the need for care and support.
- Enable earlier interventions to prevent risks escalating to the point of crisis.
- Coordinate effective and efficient safeguarding responses.
- Identify people who may pose a risk to others and if possible, work to reduce this behaviour.
- Reduce organisational risk and protect reputation.
- Prevent death or serious harm.
- Maintain and improve good practice in safeguarding adults.
- Reveal previously undetected patterns of abuse that could identify others at risk.

6. Sharing information to prevent abuse and neglect

Sharing information between organisations about known or suspected risks may help to prevent abuse taking place. Safeguarding Adults Boards have a key role to play in sharing information and intelligence on both local and national threats and risks. The Board's annual report must provide information about any safeguarding adults reviews (SARs). This can include learning to inform future prevention strategies.

7. Seven golden rules to sharing information

- 1) The UK GDPR, Data Protection Act 2018 and human rights law are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.
- 2) Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- 3) Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
- 4) Identify at least one [lawful basis](#) for sharing the data before you start sharing it. Where you are relying on consent, ensure that it is fully informed and freely given. As long as it does not increase risk, practitioners should inform the person if they need to share their information without consent.
- 5) Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
- 6) Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
- 7) Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

8. Legal basis for sharing information

8.1 Care Act 2014

The [statutory guidance to the Care Act](#) emphasises the need to share information about safeguarding concerns at an early stage; information-sharing agreements or protocols should be in place. Those sharing information about individuals alleged to have caused harm are responsible for ensuring that they are compliant with human rights, data protection and confidentiality requirements.

8.2 Sharing information with the Safeguarding Adult Board (SAB)

In order to carry out its functions effectively, the SAB may need access to information held by a wide range of safeguarding partners and individuals to enable or assist the SAB to fulfil its statutory functions. Section 45 of the Care Act 2014 requires that if the SAB requests information from a body or person who is likely to have information, they **MUST** share what they know with the SAB at its request. However, the information requested must be for the purpose of enabling or assisting the SAB to perform its functions.

8.3 Legislation giving powers or duties to share information

Sharing information between organisations as part of day-to-day safeguarding practice is not covered in the Care Act because it is already covered in existing legislation as follows:

Common law duty of confidentiality - Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. However, the right to confidentiality is not absolute. Sharing relevant information with the right people at the right time is vital to good safeguarding practice. All staff and volunteers should be familiar with their internal safeguarding procedures for raising concerns. They can also contact either the police or the local authority safeguarding lead for advice, without necessarily giving an individual's personal details, if they are unsure whether a safeguarding referral would be appropriate.

Human Rights Act 1998 – Under Article 8 of the European Convention on Human Rights, individuals have a right to respect for their private life. This is not an absolute right and can be overridden if necessary and in accordance with the law. Interference must be justified and be for a particular purpose. Justification could be protection of health, prevention of crime, protection of the rights and freedoms of others. A decision to share information and the reasoning behind it should be recorded.

Data Protection Act 2018 - Since the UK left the EU, the GDPR has been written into UK law as the UK GDPR, to sit alongside the Data Protection Act 2018 (DPA 2018). The law is wide-reaching and places a range of new duties and responsibilities on organisations that store data from which individuals can be identified (the Information Commissioner's Office provides detailed guidance on UK GDPR). The DPA and UK GDPR do not change practice regarding safeguarding adults because the UK GDPR, like the previous legislation, permits sharing information without consent in certain circumstances. If it is deemed to be in the public interest, data may be collected, processed, shared and stored. It may be stored for longer periods in the public interest and in order to safeguard the rights and freedoms of individuals. **Vital interests** are a lawful basis for sharing personal data to protect someone's life, but other less intrusive

ways to protect the person's life must be explored with the decision justified and documented in a record.

Crime and Disorder Act 1998 – Any person may disclose information to a relevant authority under Section 115 of the Crime and Disorder Act 1998, 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)'. 'Relevant authorities', broadly, are the police, local authorities, health authorities (clinical commissioning groups) and local probation boards.

Mental Capacity Act 2005 – The MCA is also relevant as all those coming into contact with adults with care and support needs should be able to assess whether someone has the mental capacity to make a decision concerning risk, safety or sharing information.

Each of these laws and regulations have to be considered separately when deciding whether information can be shared. In general, they do not prevent the sharing of information with other agencies / staff members if:

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

8.4 Decision-making about sharing information

Practitioners should use their judgement when making decisions about what information to share and should follow organisational procedures or consult with their manager if in doubt. The most important consideration is whether sharing the information is likely to support the safeguarding and protection of an adult with care and support needs. Decision-making will also need to take into account the following considerations:

Necessary and proportionate

When taking decisions about what information to share, practitioners should consider how much information is necessary to release. Not sharing more data than is necessary to be of use is a key element of the UK GDPR and Data Protection Act 2018 and the impact of disclosing information on the information subject and any third parties should also be taken into account. The information shared must be proportionate to the need and level of risk.

Relevant

Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

Adequate

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to an adult with care and support needs who is at risk. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place an adult at risk at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

Record

Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

8.5 What if a safeguarding partner is reluctant to share information?

There are some circumstances where it would be acceptable not to share information pertinent to safeguarding concerns with relevant safeguarding partners. These include where the person involved has the mental capacity to make the decision and does not want their information shared **and**:

- Other adults with care and support needs, or children. are not at risk.
- The person alleged to have caused the harm has no care and support needs.
- No serious crime has been or may be committed.
- Nobody in a position of trust is implicated in the concerns.
- No coercion or duress is suspected.
- The public interest served by the disclosure of information does not outweigh the public interest served by protecting confidentiality.
- The risk is not high enough to warrant a multi-agency risk assessment conference (MARAC) referral (in cases of domestic abuse).
- No other legal authority has requested the information.

Where there is continued reluctance from one partner to share information on a safeguarding concern the matter should be referred to the Local SAB. It can then consider whether the concern warrants a request, under Section 45 of the Care Act, for the 'supply of information'. Then the reluctant party would only have grounds for refusal if it would be 'incompatible with their own duties or have an adverse effect on the exercise of their functions'.

8.6 What if an adult does not want their information shared?

Staff and volunteers should always share safeguarding concerns in line with their own organisation's policy and requirements. As long as it does not increase the risk to the adult, the member of staff should explain to the adult that they have a duty to share their concern.

An adult may disagree with safeguarding information being shared. There may be a number of reasons behind this such as they may be frightened of reprisals, they may fear losing control, they may not trust social services or other partners or they may fear that their relationship with the abuser will be damaged. Reassurance and appropriate support may help the adult understand the necessity to share the information. If an adult refuses support to help them with a safeguarding concern, or requests that information about them is not shared with other safeguarding partners, their wishes should be respected where possible. However, there are a number of circumstances where there will be a duty to share information regardless of the person's wishes, including:

- Other adults with care and support needs, or children, are or may be at risk.
- The person who may have caused harm has care and support needs and may also be at risk
- People in a position of trust are implicated.
- The adult lacks the mental capacity to make that decision – this must be properly assessed and recorded in line with the Mental Capacity Act 2005.
- The adult has the mental capacity to make this decision but they may be under duress or being coerced.
- Sharing the information is necessary to prevent, detect or investigate a crime.
- A serious crime may have been committed.
- The domestic abuse risk is extremely high and meets the criteria for a multi-agency risk assessment conference referral (MARAC).
- A court order or other legal authority has requested the information.

If the decision is not to share safeguarding information with other safeguarding partners, or not to intervene to safeguard the adult:

- Support the adult to weigh up the risks and benefits of different options.
- Ensure they are aware of the level of risk and possible outcomes.
- Offer to arrange for them to have an advocate or peer supporter.
- Offer support for them to build confidence and self-esteem if necessary.
- Agree on and record the level of risk the adult is taking.
- Record the reasons for not intervening or sharing information.
- Regularly review the situation.

Decisions to either share safeguarding information against the wishes of the adult or NOT to share this information with safeguarding partners, must take into account the considerations outlined above and must be proportionate to the presenting risks. These decisions should be made by the organisation rather than the individual staff member and made on a case-by-case basis informed by a risk assessment. The decision and the rationale for it should be documented in order to demonstrate defensible decision-making.

If it is not clear that information should be shared outside the organisation, a conversation can be had with safeguarding partners in the police or local authority without disclosing the identity of the adult in the first instance. They can then advise on whether full disclosure is necessary against the wishes of the person concerned.

It is very important that the risk of sharing information is also considered. In some cases, such as domestic abuse or hate crime, it is possible that sharing information could increase the risk to the adult. Safeguarding partners need to work jointly to provide advice, support and protection to the individual in order to minimise the possibility of worsening the relationship or triggering retribution from the abuser.

Domestic abuse cases should be assessed using the Domestic Abuse Stalking and Harassment (DASH) Risk Identification risk assessment and referred to a Multi-Agency Risk Assessment Conference (MARAC) where appropriate. Cases of domestic abuse should also be referred to local specialist domestic abuse services in line with local pathways.

8.7 The impact of sharing or withholding information

There may be anxieties about the legal or ethical restrictions on sharing information, particularly with other agencies. There should, however, be an awareness of relevant legislation and agencies and their practitioners should also comply with their professional codes of conduct, the 4LSAB Multi-agency Procedures and other relevant agency guidance. These rarely provide an absolute barrier to disclosure. A failure to pass on information that might prevent a person at risk from being abused or a more serious tragedy could expose agencies/staff to criticism in the same way as an unjustified disclosure.

8.8 Managing Allegations against People in a Position of Trust

It is a requirement under the Care Act 2014 for the local authority and its relevant partners providing universal care and support services to establish clear policies (reflecting those from the local SAB) for dealing with allegations against people in a position of trust e.g. anyone working in either a paid or unpaid capacity with adults with care and support needs. These policies should clearly distinguish between an allegation, a concern about the quality of care or practice, and a complaint. Employers should ensure that their disciplinary procedures are compatible with the responsibility to protect adults at risk of abuse or neglect.

The responsibility for addressing these concerns rests with the employer (or student body or voluntary organisation) who must risk assess any potential risks to adults who use their services and if necessary, take action to safeguard those adults. This may involve proportionate and relevant information sharing with other agencies including regulatory and professional bodies, the police and the local authority adult services as appropriate.

The Police are able to keep records on any person known to be a target or perpetrator of abuse and share such information with safeguarding partners for the purposes of protection 'under Section 115 of the Crime and Disorder Act 1998, and the Data Protection Act 2018, provided that criteria outlined in the legislation are met'. All police forces now have IT systems in place to help identify repeat and vulnerable victims of anti-social behaviour.

8.9 Referring to the Disclosure and Barring Service

The Safeguarding Vulnerable Groups Act 2006 places specific duties on those providing 'regulated' health and social care activities. They must refer to the Disclosure and Barring Service (DBS) anyone who has been dismissed or removed from their role because they are thought to have harmed, or pose a risk of harm to, a child or adult with care and support needs. This applies even if they have left their job and regardless of whether they have been convicted of a related crime.

8.10 Professional codes of practice

Many professionals, including those in health and social care, are registered with a Professional Body and governed by a code of practice or conduct. These codes often require those professionals to report any safeguarding concerns in line with legislation. The statutory guidance to the Care Act 2014 requires all organisations in contact with people with care and support needs to have in place an allegations management process that enables referrals of individual employees to regulatory bodies to be made promptly and appropriately. The regulatory bodies for the main health and social care professionals are as follows:

- Social Work England (SWE)
- Nursing and Midwifery Council (NMC)
- General Medical Council (GMC)
- Health and Care Professions Council (HCPC)

Each Professional Body regulates the standards within the profession for which they are responsible and requires all those registered with that body to comply with a professional duty to take appropriate and timely action to address and report concerns about safety or wellbeing of people using services, follow up concerns, and be open and honest if things go wrong. It may be necessary to share information with the relevant professional body any 'Fitness to Practice' concerns or the outcomes of anyone who has been dismissed or removed from their role because they are thought to have harmed, or pose a risk of harm to, a child or adult with care and support needs. This applies even if they have left their job and regardless of whether they have been convicted of a related crime.

8.11 Duty of Candour

The Duty of Candour requires all health and adult social care providers registered with the Care Quality Commission (CQC) to be open with people when things go wrong. The regulations impose a specific and detailed duty on all providers where any harm to a service user from their care or treatment is above a certain harm threshold.

The Duty of Candour is a legal requirement and CQC will be able to take enforcement action when it finds breaches. The Duty requires providers to offer an apology and state what further action the provider intends to take in this situation. In practice, this means that care providers are open and honest with patients when things go wrong with their care and treatment. If the provider fails to comply with the Duty, CQC can move directly to prosecution without first serving a warning notice. This policy embraces this Duty in relation to safeguarding adults, and all Section 42 enquiries and safeguarding processes must check that this Duty has been fulfilled.

The regulations also include a more general obligation on CQC registered providers to 'act in an open and transparent way in relation to service user care and treatment'. This means that the default position should be to be open, honest and candid, unless there are justifiable reasons for not being so – for example because the service user actively says that they do not want further information about the incident. However, these circumstances should be the exception rather than the norm. Further information can be found at [Duty of Candour](#).

8.12 Commissioning

Commissioners of care and support services should consider whether contracts should place an obligation on service providers to share safeguarding information. Any specifications would need to be in line with policy, regulation and the law. More information can be found here: [Guidance on Safeguarding in Commissioned Services](#).

8.13 Multi-Agency Safeguarding Hubs

Some local areas have a Multi-Agency Safeguarding Hub (MASH), which formalise arrangements for information sharing in the safeguarding context. The purpose is to ensure that relevant information about potential safeguarding concerns in respect of adults and children is shared appropriately by the partner agencies where necessary. This enables the level of risk to be assessed appropriately and allows for suitable responses to be agreed.

MASH models will require separate information sharing agreements and protocols to be put in place to provide the basis for sharing information between the agencies engaged in the MASH in order to facilitate and govern the efficient, effective and secure sharing of timely and accurate information. It is acknowledged that the disclosure of any personal data must be bound to both common law and statute, for example defamation, the common law duty of confidence, the Data Protection Act 2018 and the Human Rights Act 1998.

9. Confidentiality

Agencies should draw up a common agreement relating to confidentiality and setting out the principles governing the sharing of information, based on the welfare of the adult or of other potentially affected adults. Any agreement should be consistent with the principles set out in the Caldicott Review published 2013 ensuring that:

- Information will only be shared on a 'need to know' basis when it is in the interests of the adult. Confidentiality must not be confused with secrecy.
- Agreement to share should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to disclose information; and
- It is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk.

Where an adult does not want information disclosed for these purposes, then practitioners must consider whether there is an overriding public interest that would justify information

sharing (e.g. because there is a risk that others are at risk of serious harm) and wherever possible, the appropriate Caldicott Guardian should be involved in the decision-making. In these circumstances it would be good practice to only share information against the person's wishes in the context of a documented risk assessment.

Decisions about who needs to know and what needs to be known should be taken on a case by case basis, within agency policies and the constraints of the legal framework. Principles of confidentiality designed to safeguard and promote the interests of an adult 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 welfare of an adult. If it appears to an employee or person in a similar role that such confidentiality rules may be operating against the interests of the adult then a duty arises to make full disclosure in the public interest.

Exchange or disclosure of personal information must be made in accordance with the law on confidentiality and the Data Protection Act 2018 where this applies. The Home Office and the Information Commissioner's Office have issued general guidance on the preparation and use of information sharing protocols. The Caldicott principles provide the basis of ethical and appropriate information sharing.

10. Recording

10.1 Record keeping

Good record keeping is a vital component of professional practice. Whenever a complaint or allegation of abuse is made, all agencies should keep clear and accurate records and each agency should identify procedures for incorporating, on receipt of a complaint or allegation, all relevant records into a file to record all action taken. When abuse or neglect is raised, managers should look for past incidents/concerns in order to identify repeating or escalating risks and patterns.

In the case of providers registered with CQC, records of these should be available to service commissioners and the CQC so they can take the necessary action. Staff should be given clear direction as to what information should be recorded and in what format. The following questions are a guide to recording practice:

- What information do staff need to know in order to provide a high-quality response to the adult concerned?
- What information do staff need to know in order to keep adults safe under the service's duty to protect people from harm?
- What information is not necessary?
- What is the basis for any decision to share (or not) information with a third party?

Records should be kept in such a way that the information can easily be collated for local use and national data collection.

Individual agencies should establish arrangements, consistent with principles and rules of fairness, confidentiality and data protection, to make records available to those adults affected by, and subject to, a safeguarding enquiry. If the alleged abuser is using care and support themselves then information about their involvement in an adult safeguarding enquiry, including the outcome, should be included in their case record. If it is assessed that the individual continues to pose a threat to other people then this should be included in any information that is passed on to service providers or other people who need to know.

10.2 Safeguarding meetings and notes

In order to safeguard a person with care and support needs who is at risk, it may be necessary to share confidential information during a safeguarding meeting. It is the responsibility of the Chair of that meeting to request any relevant information and to secure the agreement of the relevant parties to sharing this information.

The Chair of the meeting will ensure that a confidentiality statement is made at the start of the meeting and all parties understand their responsibilities in respect of confidentiality. Exchange may be verbal or written. However, data protection principles must still apply with attendees only being present where it is appropriate for them to share the information.

Any notes taken at the meeting will be marked 'OFFICIAL SENSITIVE' or 'OFFICIAL SENSITIVE - NOT FOR CIRCULATION'. Only those practitioners who are invited to the meeting will receive copies of the notes. Wherever possible, the adult should also be provided with a copy of the meeting notes.

10.3 Access to records

Individual requests for access to records will be considered in line with the Data Protection Act and Departmental Policy.

Requests for access to the notes/minutes of safeguarding adult meetings should be considered on a case by case basis and be consistent with Freedom of Information Act 2000, UK GDPR, Data Protection Act 2018 and in line with individual agency information governance policies. Information can only be disclosed if it is appropriate to do so.

For further advice, contact should be made with the Data Protection/Information Governance/Compliance officer or Freedom of Information officer from the relevant organisation, or contact can be made with the Information Commissioner.

If an organisation wishes to disclose confidential information, permission (i.e. consent) must be obtained in writing from the initial owner of the information. If this may not be appropriate, then prior advice should be sought from the Data Protection/Information Governance/Compliance officer or Freedom of Information officer from the relevant organisation, or contact can be made with the Information Commissioner.

11. The Caldicott Principles

The 8 Caldicott Principles were published in December 2020

Principle 1: Justify the purpose(s) for using confidential information. Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary. Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information. Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis. Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities. Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law. Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used. A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

12. Links to relevant information

For more information on information sharing please use the links below:

[Care Act 2014 Statutory Guidance Chapter 14 - Safeguarding](#)

[SCIE Guidance on Information Sharing](#)

[Data sharing: a code of practice | ICO](#)