

Bristol Safeguarding Adults Board
Listening learning leading



Bristol Safeguarding Adults Board

Information Sharing Guidance

Contents

- 1. Guidance on information sharing 3
- 2. Key Messages..... 3
- 3. The seven golden rules to sharing information..... 5
- 4. Powers or obligations to share information for adult safeguarding 5
 - a) Referring to the Disclosure and Barring Service 5
 - b) Professional codes of practice 6
 - c) Duty of Candour 6
 - d) Commissioners 6
 - e) Sharing information on prisoners 6
 - f) Sharing information on those who may pose a risk to others 7
 - g) Multi Agency Safeguarding Hubs..... 7
- 5. Information sharing agreements and protocols..... 7
- 6. Key principles in line with Sharing Information under The Care Act 2014..... 8
 - a) Record-keeping 8
 - b) Confidentiality 9
 - c) The Caldicott Principles..... 10
- 7. Training 11
- 8. Review 11
- 9. Links to information..... 11

Bristol Safeguarding Adults Board
Listening learning leading

1. Guidance on information sharing

Sharing the right information, at the right time, with the right people, is fundamental to good practice in safeguarding adults, although this is often complex. 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.

This guidance is aimed at supporting partner organisations to understand their roles and responsibilities and to co-operate with one another to share information for safeguarding purposes in accordance with the statutory guidance provided by the Act. This guidance does not supercede single agency information sharing arrangements where the decision to share personal and sensitive data rests with each organisation, in accordance with the Data Protection Act 1998. It deals with information sharing in relation to Bristol Safeguarding Adults Board (BSAB) business.

The BSAB and partner agencies will need to share strategic information to improve local safeguarding practice and ensure that partner agencies understand their duty to comply with requests for information from the Board (Section 45 'the supply of information'). This guidance covers information sharing in a range of contexts relating to adult safeguarding including:

- Raising concerns and making referrals about abuse or neglect (or risk of this of an adult with care and support needs)
- Undertaking and sharing the outcomes of safeguarding enquiries
- Responsibilities to share information and make referrals to DBS and/or professional bodies
- Exchange information in the context of allegation management with the relevant Safeguarding Adult Lead Manager
- Exchange information between the Local Authority Safeguarding Adult Lead Manager and the Local Authority Designated Officer concerning children
- Sharing qualitative and quantitative data for the purpose of informing the work of the safeguarding adults board
- Share information arising from the context of a Safeguarding Adult Review or other form of multi-agency learning review.

2. Key Messages

- 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 reasonably be overridden in certain circumstances including:
 - the person lacks the mental capacity to make that decision – this must be properly explored and recorded in line with the Mental Capacity Act
 - other people are, or may be, at risk, including children

- sharing the information could prevent a crime
- the alleged abuser has care and support needs and may also be at risk
- a serious crime has been committed
- staff are implicated
- the person has the mental capacity to make that decision but they may be under duress or being coerced
- the risk is unreasonably high and meets the criteria for a multi-agency risk assessment conference referral
- a court order or other legal authority has requested the information.
- Emergency or life-threatening situations may warrant the sharing of relevant information with the relevant emergency services without consent.
- 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 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.
- The Data Protection Act enables the lawful sharing of information.
- There should be a local agreement or protocol in place setting out the processes and principles for sharing information between organisations.
- 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 consent to share information.
- As long as it does not increase risk, practitioners should inform the person if they need to share their information without consent.
- Organisational policies should have clear routes for escalation where a member of staff feels a manager has not responded appropriately to a safeguarding concern.
- All organisations must have a whistleblowing policy.
- The management interests of an organisation should not override the need to share information to safeguard adults at risk of abuse.
- All staff, in all partner agencies, should understand the importance of sharing safeguarding information and the potential risks of not sharing it.

- All staff should understand when to raise a concern with the local authority adult social services.
- The six safeguarding principles should underpin all safeguarding practice, including information-sharing.

3. The seven golden rules to sharing information

1. Remember that the Data Protection Act 1998 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 data controller if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
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.

4. Powers or obligations to share information for adult safeguarding

a) 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. The statutory guidance to the Care

Act 2014 requires Safeguarding Adult Lead Managers to work with partner agencies to ensure that referral of individual employees to the DBS is carried out promptly and appropriately.

b) Professional codes of practice

Many professionals, including those in health and social care, are registered with a 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 Safeguarding Adult Lead Managers to work with partner organisations to ensure that referrals of individual employees to regulatory bodies are made promptly and appropriately.

c) Duty of Candour

The obligations associated with the statutory Duty of Candour are contained in regulation 20 of The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014. The Duty of Candour was introduced for NHS bodies in England (trusts, foundation trusts and special health authorities) from 27 November 2014, and applies to all other care providers registered with CQC from 1 April 2015.

It places a duty on organisations to act in an open and transparent way in relation to care provided to individuals. 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.

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. Safeguarding processes must check that this Duty has been fulfilled.

If the provider fails to comply with the Duty, CQC can move directly to prosecution without first serving a warning notice.

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 Candour¹

d) Commissioners

Those commissioning 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. Individual agencies should have policies in place to deal with this.

e) Sharing information on prisoners

The statutory guidance to the Care Act 2014 requires Local Authorities to share information about people with care and support needs in, or in transition from or to, prison or custodial settings. This includes '*the sharing of information about risk to the prisoner and others where this is relevant*'.

f) Sharing information on those who may pose a risk to others

The Police can 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 1998, 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 antisocial behaviour.

The statutory guidance to the Care Act 2014 states that Safeguarding Adults Boards should:

“have a framework and process for any organisation under the umbrella of the SAB to respond to allegations and issues of concern that are raised about a person who may have harmed or who may pose a risk to adults”.

Safeguarding Adult Lead Managers should 'ensure the control of information in respect of individual cases is in accordance with accepted Data Protection and Confidentiality requirements'.

g) Multi Agency Safeguarding Hubs

The establishment of Multi Agency Safeguarding Hubs (MASH) 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.

As the MASH model is implemented more widely locally, separate information sharing agreements and protocols will need to be arranged 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 1998 and the Human Rights Act 1998.

5. Information sharing agreements and protocols

It is good practice to have an information sharing agreement in place when sharing personal and sensitive personal data on a regular basis between organisations.

An information sharing agreement is a set of rules governing the processing of the shared information, it does not create any additional powers or legal gateways.

The lack of an information sharing agreement does not prevent the legitimate sharing of information. Ad hoc sharing or 'one off requests' do not normally lend themselves to a formal informal sharing agreement.

This framework acknowledges that information sharing agreements and protocols are useful tools which enable inter-agency communication, facilitate effective partnership working and support decision making. Local agencies will put in place appropriate agreements to address key points to an agreed standard from the Data Sharing Code of Practice including:

- The information that needs to be shared is disclosed and transferred securely

- The justification for sharing personal information
- Organisations that will be involved
- What people need to be told about the data sharing and how this information will be communicated
- Measures to ensure adequate security is in place to protect data in its collection, storage, use, sharing, transfer and disposal
- Arrangements to provide individuals with access to their personal data if requested
- Agreed common retention periods for the data where it is held no longer than is necessary. This information needs to be reviewed, its purpose considered, updated, archived and deleted securely as it goes out of date or is no longer needed
- Processes to ensure secure deletion takes place.

6. Key principles in line with Sharing Information under The Care Act 2014

a) 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 need to look for past incidents, concerns, risks and patterns. We know that in many situations, abuse and neglect arise from a range of incidents over a period of time. 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 collections.

All agencies should identify arrangements, consistent with principles and rules of fairness, confidentiality and data protection for making records available to those adults affected by, and subject

to, an 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.

The Care Act 2014 establishes the importance of organisations sharing vital information related to abuse or neglect with the Safeguarding Adult Board (SAB). In order to carry out its functions effectively, the SAB may need access to information that a wide number of people or other organisations hold in order to enable or assist the SAB to do its job.

Section 45 of the Act ensures 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. But only if the information requested is for the purpose of enabling or assisting the SAB to perform its functions. The body or person requested to supply the information must have functions or engage in activities of a nature that the SAB considers it likely that they have information relevant to a function of the SAB.

b) Confidentiality

All agencies will agree to the principles governing the sharing of information, based on the welfare of the adult or of other potentially affected adults which is 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
- Informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement; 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 has refused to consent to information being 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 without consent 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, disclosure, storage and retention of personal information must be made in accordance with the law on confidentiality and the Data Protection Act 1998 where this applies. The Home Office and the Office of the Information Commissioner 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.

c) The Caldicott Principles

Based on the findings of the Information Governance Review – To Share or Not to Share?

1. **Justify the purpose(s).** Every single 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.
2. **Don't use personal confidential data unless it is necessary.** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for adults to be identified should be considered at each stage of satisfying the purpose(s).
3. **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 information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis.** Only those individuals who need access to personal confidential information should have access to it, and they should only have access to the information 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.
5. **Everyone with access to personal confidential data should be aware of their responsibilities.** Action should be taken to ensure that all those handling personal confidential data are made fully aware of their responsibilities and obligations to respect individuals' confidentiality.
6. **Understand and comply with the law.** Every use of personal confidential information must be lawful. Someone in each organisation handling personal confidential information should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect confidentiality.** Health and social care professionals and other staff should have the confidence to share information in the best interests of adults within the framework set out by these principles. Official policies should support them doing so.

7. Training

It is important that all organisations ensure that staff engaged in information sharing receive appropriate training and support to enable them to share information confidently and proportionately to prevent harm and reduce risk.

Where possible, joint training and use of common training materials should be encouraged between organisations, to help break down barriers, build trust, and support confident and consistent information sharing between organisations to prevent harm and reduce risk.

8. Review

This Guidance will be reviewed in 2017 by the Executive Board.

9. Links to information

For more information on information sharing:

¹Duty of Candour

<http://www.themdu.com/guidance-and-advice/guides/statutory-duty-of-candour/statutory-duty-of-candour#sthash.3xOBNeTG.dpuf>

<http://www.cqc.org.uk/content/regulation-20-duty-candour>

²SCIE Guidance on Information Sharing:

<http://www.scie.org.uk/care-act-2014/safeguarding-adults/sharing-information>

³Government Guidance on Information sharing, 2015 - advice about information sharing, for people who provide safeguarding services to children, young people, parents and carers.

<https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>