Hertfordshire
Safeguarding Adults Board
Working together to prevent abuse

Information sharing

The policy of Hertfordshire Safeguarding Adults Board is that information to safeguard and promote the welfare of individuals will be shared between agencies on a need to know basis in line with both the statutory guidance and the Information Sharing Agreement and Protocol for HSAB.
It is important to identify any potentially abusive situation as early as possible so that the individual can be protected. Withholding information may lead to abuse not being dealt with in a timely manner. Confidentiality must never be confused with secrecy.

In seeking to share information for the purposes of protecting adults at risk, agencies are committed to the following principles:

- personal information will be shared in a manner that is compliant with agencies statutory responsibilities;
- adults at risk will be fully informed about information that is recorded about them and as a general rule, be asked for their permission before information about them is shared with colleagues or another agency. However, there may be justifications to override this principle if the adult or others are at risk;
- staff will receive appropriate training on service users/patient confidentiality and secure data sharing;
- the principles of confidentiality designed to protect the management interests of an organisation must never be allowed to conflict with those designed to promote the interests of the adult at risk.

Aggregated/statistical data may also be shared between agencies to:
- coordinate partnership working and improve delivery of services;
- train staff and set professional standards;
- manage, plan, commission and contract services;
- develop inter-agency strategies;
- improve performance management and audit;
- inform local and national research initiatives.

However, this data will not identify any individual.

Procedure

There is an Information Sharing Agreement in place which identifies the purposes and statutory basis for the work of the Hertfordshire Safeguarding Adults Board. All agencies will also have internal policies and procedures in respect of information sharing and data security in compliance with the Data Protection Act and Caldicott principles which staff should follow when they are sharing information.

Caldicott principles

Principle 1. Justify the purpose(s) for using confidential information
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 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 patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 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 data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4. 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 5. 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 responsibilities and obligations to respect patient confidentiality.

Principle 6. 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 7. 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 patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principles guiding the sharing of information

The three main sources of law on confidentiality which allow for information to be disclosed in certain circumstances, even if consent has been refused, are set out in the section ‘relevant legislation and guidance’:

- safeguarding and promoting the welfare of individuals is the prime consideration in all decision making about information sharing;
- safeguarding adults work requires the sharing of personal information, both about an adult at risk and a person who (may have) caused harm;
- workers should share as much information as is required to address the safeguarding issue;
- withholding information may lead to abuse not being dealt with in a timely manner.

Explicit consent is not always necessary to share personal and sensitive personal information as there are circumstances when information can be shared even if consent is explicitly withheld. For example:

- a serious crime may have been committed;
- where the person who caused harm may harm other adults at risk;
- other adults are at risk;
- the adult is deemed to be at serious risk of harm;
- there is a statutory requirement e.g. Children's Act 1989, Mental Health Act 1983, Care Standards Act 2000;
- the public interest in sharing the information overrides the interest of the individual.

It is best practice to gain the permission of the adult at risk before sharing information about them where capacity and security is not a concern. 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.

If a practitioner considers that an adult may not have the capacity to give permission for their information to be shared, the *Mental Capacity Act 2005 and its Code of Practice* must be followed. When requesting/providing information workers and managers should clearly record:

- why the information is being sought and that the request is part of the safeguarding adults from abuse procedure;
- why it cannot be accessed in another way or by consent and the exact nature of the information that has been disclosed.

Consideration should be given to the following questions before making a decision on whether to disclose information without the consent of the adult at risk:

- what risks will others face if the information is not disclosed, including the risk of self-harm to the adult at risk;
- will the rights and freedoms of the public be affected if it isn't disclosed;
- will a crime be committed;
- will the investigation of a crime be hampered;
- is there another, equally effective way, of achieving the same aim without disclosing personal information without consent;

- what is the impact of the disclosure likely to be on the person who is the subject of the information? Is this out of proportion to the benefit of disclosing the information.

If there is any doubt as to whether confidential information about an adult at risk should be disclosed to a third party, then legal advice should be obtained.

All partner agencies should also ensure that any information that they obtain /share is held securely and destroyed after use or other appropriate retention period.

Security of information

Ensuring the security and accuracy of confidential information is the responsibility of management and staff at all levels. Partner agencies must ensure that they have in place methods of accurately recording information and that:

- manual and computer records containing such information is kept secure and care is taken to avoid any unintentional breach of confidentiality;
- any breach of confidentiality is considered to be a serious matter and will be dealt with under each a relevant personnel policy;
- one of the offences under the Data Protection Act 2018 which has particular significance for staff is that it is an offence to knowingly or recklessly obtain or disclose personal or patient identifiable information without the consent of the data controller, this covers unauthorised access to and disclosure of personal/patient identifiable information.

Relevant legislation and guidance

The law allows for information to be disclosed in certain circumstances even if consent has been refused.

Common Law

The starting position is that personal information provided in confidence can only be disclosed without consent when it is in the public interest to do so and there must also be a pressing need for the disclosure to occur.

Public interest includes the protection of ‘at risk’ members of the community and maintaining public safety

The main pieces of legislation which set this out are:

- Human Rights Act 1998 – namely Article 2 [The Right to Life] and 8 [The right to respect for Private and Family Life}
- Data Protection Act 1998
- Common Law duty of confidentiality
- Care Act 2014

Other relevant legislation and guidance can also be found in:

- Care and Support Statutory Guidance Crime and Disorder Act 1998 – Section 115
- The 1997 Caldicott Report.
- The 2013 Caldicott Report *Information: to share or not to share* also known as Caldicott 2.

The Data Protection Act 2018

The Data Protection Act 2018 allows for the disclosure of personal and sensitive personal information without the consent of the individual concerned if it is necessary for:

- the performance of a contract to which the data subject is a party
- to comply with any legal obligation other than one imposed by contract
- to protect the vital interests of the data subject
- for the administration of justice/for the exercise of any functions conferred by or under an enactment/for the exercise of a function by the Crown, a Minister of the Crown or a government department or for the exercise of any other function of a public nature exercised in the public interest by any person
- for the purposes of legitimate interests pursued by the controller of the data or to any third party to which it is disclosed
- for the purposes of legal proceedings, obtaining legal advice or exercising/defending legal rights
- for medical purposes.

Personal data must be:

- processed lawfully
- processed for specific purposes
- adequate, relevant, not excessive
- accurate and up to date
- not kept for longer than necessary
- processed in accordance with the rights of the data subject
- protected by appropriate security
- not transferred outside the EEA (European Economic Area) without adequate protection

The Human Rights Act 1998, Article 2 [Right to Life]

The Human Rights Act 1998, Article 2 states that “everyone’s right to life shall be protected by law”. Case law has developed to a point where a positive obligation has been placed on public authorities to actively protect the vulnerable from the risk of self-harm. In light of this, depending on the circumstances of the case, we could have a duty to share information to protect life.

The Human Rights Act 1998, Article 8

The Human Rights Act 1998, Article 8 allows a public authority to interfere with the privacy of an individual if the interference 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 disorder or crime, for

the protection of health and morals, or for the protection of the rights and freedoms of others

Record keeping and confidentiality

Organisations will have their own recording systems for keeping comprehensive records whenever a concern is made/arises/occurs, and of any work undertaken under the safeguarding adult's procedures, including all concerns received and all referrals made. Organisations should refer to their own internal policies and procedures for additional guidance on recording and storage of records.

Throughout the safeguarding adult's process, detailed factual records must be kept. This includes the date and circumstances in which conversations and interviews are held and a record of all decisions taken relating to the process.
Records may be disclosed in court as part of the evidence in a criminal action/case or may be required if the regulatory CQC authority decides to take legal action against a provider.

Records kept by providers of services should be available to service commissioners and to regulatory authorities.

Agencies should identify arrangements, consistent with the principle of fairness, for making records available to those affected by, and subject to, investigation with due regard to confidentiality.