

7 INTER-AGENCY PROTOCOLS – SHARING OF INFORMATION:

- 7.1 Sharing personal and confidential information lawfully between agencies is essential when protecting vulnerable adults from abuse. The general principles for achieving this are:
- The informed consent of the vulnerable person should be obtained when ever possible (See paragraph 8.16 section 8: ‘Consent – the Basic Principles’ for meaning of the term ‘informed consent’)
 - Sharing information should be on a ‘need to know basis’ only
 - Vulnerable adults should be informed from the outset what the limits and boundaries of confidentiality are.
 - Where possible, the vulnerable adult should be kept informed of what personal information about them is being shared with other agencies or individuals
- 7.2 **Practitioners and Managers should always remember** – the promise of complete confidentiality should not be given to the person reporting the referral or raising the ‘concern’ – this includes the vulnerable adult.
- 7.3 When such information is passed to Social Services, Health, CSIW or the Police, these agencies are likely to take positive action. This applies even if consent has not been given in circumstances such as:
- The vulnerable adult is believed to lack capacity to make informed choice
 - A criminal investigation by the police is warranted
 - A wider public interest exists
- 7.4 In furtherance of this, each partner agency must have their own policies and procedures for ensuring that vulnerable adults receive a confidential service. It is therefore, important that staff have due regard to their own agency’s policies when dealing with issues of confidentiality in the context of their work regarding the abuse of vulnerable adults.
- 7.5 The question of sharing or disclosing information with a view to protecting vulnerable adults presents a number of professional, ethical, practical and legal dilemmas. Any disclosure of information must be bound to both common and statute law, for example the common law duty of confidence, the Data Protection Act 1998, the Public Interest Disclosure Act 1998, the Human Rights Act 1998 and the Care Standards Act 2000. (For further details of these provisions, see Section 14: Legal Context).

- 7.6 In recognising the need to support and enable staff to work confidently with shared information without fear of ‘breaking the rules’, the Welsh Assembly Government is in the process of developing ‘**Confidentiality: Codes of Practice for Health and Social Care in Wales**’ which is expected to be published shortly. It is expected that this guidance will provide a common set of rules for handling information safely and should be of considerable assistance in compiling Information Sharing Protocols relevant to information sharing across all agencies involved in the care, support and protection of vulnerable adults.
- 7.7 In the context of sharing confidential information, the issue of consent is extremely important and must be understood. Further guidance on ‘Consent – the basic principles’ can be found in paragraphs 8.16-19, Section 8: Capacity and Consent, and also in Section 14: Legal Context, paragraph 14.68 which relates to the sharing of information between agencies in compliance with the Human Rights Act.
- 7.8 It will always be difficult to make decisions about whether to share (or not to share) information about risk, particularly where the issue is about disclosing to individuals or voluntary bodies. It will always be crucial to gather the best information possible about the risk posed, assess the risk and consult thoroughly before reaching a decision.
- 7.9 **Key principles for managing information:**
- 7.10 There are a number of key principles for managing information concerning service users in multi-disciplinary work with vulnerable adults:
- Information given to an individual member of staff or agency representative belongs to the agency and not the individual employee. Therefore, decisions to share information about a service user with other agencies, without the consent of the service user in question, must be made by the agency and not one individual acting on their own.
 - Decisions made to share information concerning the service user with other agencies can normally only be made with the expressed consent of the service user (See paragraphs 7.11 – 7.16 relating to Confidentiality)
 - Although the views and wishes of the service user will normally be respected when sharing information they give us agencies cannot guarantee a fully confidential service. There will always be exceptional circumstances when a duty to protect the wider public interest will outweigh the responsibility to any one individual (see paragraph 8.20, Section 8: Capacity and Consent – ‘Best Interests’ of the vulnerable adult).

- Information given to an agency must only be used for the purposes for which it was intended.
- Service users and where appropriate carers, must be advised as early as possible why and with whom information will be shared. Best practice should encourage user and carer participation in the process of information sharing.
- Information about service users and carers must only be shared within an agency on a need to know basis to support the effective delivery of services of that user. 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.
- Staff have a clear duty to report any concerns they may have relating to the abuse or suspected abuse of a vulnerable adult to their line manager at the earliest opportunity.

7.11 **Confidentiality:**

- 7.12 Principles of confidentiality designed to safeguard and promote the interests of service users and patients are paramount. These should never be secondary or confused to protect the management interests of an organisation. Whilst these have a legitimate role, they must never be allowed to conflict with the interests of service users and patients.
- 7.13 If it appears to an employee or person in a similar role that such confidentiality may be operating against the interests of vulnerable adults then a duty exists to make full disclosure in the public interest.
- 7.14 Confidentiality must never be confused with secrecy. Whilst it will be the responsibility of participating staff to protect the confidentiality of the information that may be exchanged, in cases where non-disclosure of information may have a significant influence on the future safety of an individual or the wider public, the intentional withholding of information cannot be defended on the grounds of confidentiality.
- 7.15 Where it is necessary to disclose or exchange personal/patient identifiable information, the exchange/disclosure must always be undertaken in accordance with the principles of the Data Protection Act 1998. These state that the information/data must be:
- Processed fairly and lawfully;
 - Processed for limited purposes and in an appropriate way;
 - Relevant and sufficient for the purpose;
 - Accurate;
 - Kept for as long as is necessary and no longer;
 - Processed in line with individual's rights;

- Secure;
- Only transferred to other countries that have suitable data protection controls.

See paragraphs 14.71-76 for further information on this.

7.16 The Home Office and the Office of the Information Commissioner (formerly known as the Data Protection Commissioner) have issued general guidance on the preparation and use of information sharing protocols.

7.17 **Patient-Identifiable Information:**

7.18 **Protecting and Using Patient Information**

Patients have a right to expect that personal and sensitive information will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care.

7.19 Following a formal review of the ways in which the NHS handled and shared patient information with other organisations, the review committee chaired by Dame Fiona Caldicott, made 16 recommendations, one of which was the appointment of a Caldicott Guardian in every NHS organisation to safeguard the confidentiality of patient identifiable information.

7.20 The recommendations were translated into guidance for NHS organisations in '**Protecting and Using Patient Information: A Manual for Caldicott Guardians**'. The manual and all other work on confidentiality is underpinned by the Caldicott Principles of good practice.

7.21 **Patient Identifiable Information defined**

Patient identifiable information can be defined as all personal information about members of the public held in whatever form by or for NHS bodies or staff. It includes personal non-health information e.g. name, address and details of financial or domestic circumstances.

Sensitive personal data is a defined category under the Data Protection Act. It is information relating to physical or mental health, sexual life, racial or ethnic origin, political opinion, religious beliefs, trade union membership and data about the commission or alleged commission of an offence or disposal of criminal proceedings against someone.

It does not have to contain any clinical data in order to be sensitive. Such information might include one or more of the following patient's details:

- Address
- Surname
- Other dates
- Gender
- Forename
- Initials
- NHS number
- NI number
- Post code
- Date of birth
- Ethnic group
- Occupation

7.22 **The Caldicott Principles summarised**

- Justify the purpose(s) for using confidential information.
- Only use patient identifiable information when absolutely necessary (for some purposes aggregated data or non-personalised data may be sufficient).
- Use the minimum data required - e.g. the NHS number, or post-code may be sufficient without name, address, date of birth etc.
- Access should be on a need to know basis what means that only those who need to know should have access - e.g. managers may need to know less than their staff.
- Everyone must understand their responsibilities with regard to confidentiality – e.g. ensuring that patient identifiable information is kept secure by using password protection on computers.
- Understand and comply with the law.

7.23 **Legal requirements for keeping Patient Identifiable Information confidential**

7.24 Every NHS organisation and all NHS employees and those carrying work out on behalf of the NHS have a legal duty of confidence to patients. Health and Social care professionals also have a professional code and ethical duties of confidence. The Computer Misuse Act criminalises some activities and there are statutory restrictions relating to fertility treatment and sexually transmitted diseases.

7.25 Unauthorised disclosure of information by members of staff or by people working under contract to the NHS is a serious matter. If you breach confidentiality you could be subject to disciplinary action. Legal action is also a possibility and if you are a health professional you may find that action is taken against you by your regulatory body.

7.26 **Responsibilities of NHS organisations and its staff to maintain confidentiality**

7.27 Every NHS organisation, e.g. Local Health Boards and Trusts within the South Wales region will have appointed a Caldicott Guardian. GP practices have also been asked to nominate a

lead person to deal with the LHB Caldicott Guardian. The role of your Guardian is to raise awareness of confidentiality issues and lead your organisation in improving the protection of patient information.

7.28 One aspect of the Guardian's role is to oversee an audit of activity in the area of security and confidentiality. Every year the organisation is required to develop an action and improvement plan to move the organisation forward and then to report outcomes.

7.29 **Obtaining personal information from the Department of Work and Pensions**

7.30 The Department of Work and Pensions (DWP) is an umbrella organisation which includes the executive agencies of the Pension Service and Jobcentre Plus – both of which are regulated by the Social Security Administration Act 1992 (for further information - see Section 6: Roles of Key Agencies). The manner in which the DWP protects personal information and allows it to make disclosure of personal information to third party organisations is regulated by the Data Protection Act, Human Rights Act and common law. Currently, formal arrangements exist at a national level between the DWP and all Social Service Authorities to exchange confidential information relating to vulnerable adults – these data sharing powers being underpinned by Social Security legislation.

7.31 Additionally, a memorandum of understanding between DWP and the Association of Chief Police Officers sets out the ways in which the disclosure of personal information between the DWP and the Police can be achieved.

7.32 Whilst current arrangements imposes constraints on the disclosure of personal information to any agency other than the Social Services and Police, those agencies involved in the strategic process relating to an alleged/potential abuse of a vulnerable adult will be able to access this information through either the Social Services and/or Police. This will be on a 'need to know' basis and subject to security constraints imposed by the DWP.

7.33 **Security of Information:**

7.34 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 confidence to third parties.

7.35 Any breach of confidentiality is considered to be a serious matter and will be dealt with under each organisations relevant personnel policy.

7.36 Offences under the Data Protection Act 1998 are detailed in Section 14: Legal Context - paragraph 14.76. One of these offences, 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.

7.37 **If there is any doubt as to whether confidential information about any individual should be disclosed to a third party, then you should seek legal advice.**