

## Appendix Two: Information Governance

People have a right to know how information will be used and the right to restrict the use of information when exercising choice and control over how they are safeguarded. This may impact on the service that they are offered but it is their right to make an informed choice.

Information Governance is subject to a range of legislation, in particular the:

- [Local Authorities \(Goods and Services\) Act 1970](#)
- [Data Protection Act 1998](#)
- [Human Rights Act 1998](#)
- [Public Interest Disclosure Act 1998](#)
- [Freedom of Information Act 2000](#)
- [Mental Capacity Act 2005](#)
- [Health and Social Care Act 2008](#)
- [The Local Authority Social Services and National Health Services Complaints \(England\) \(Amendment\) Regulations 2009](#)

Practitioners must be mindful that the information that they collect is lawful and that people are routinely informed about why the information is collected, what will be done with the information and who it is likely to be shared with.

A Berkshire wide [Information Sharing Protocol](#) has been developed.

Information management requires organisations to have policies and procedures in line with the above.

Local authorities and the NHS are required to appoint a [Caldicott Guardian](#) to advise and manage its information governance arrangements.

### **Data Protection**

The Data Protection Act 1998 applies to all organisations in the UK that processes personal information. The Act goes hand-in-hand with the common law duty of confidence and professional and local confidentiality codes of practice to provide individuals with a statutory route to monitor the use of their personal information.

In the UK the Information Commissioner is responsible for the enforcement of the [Data Protection Act 1998](#) and [Freedom of Information Act 2000](#). Advice and guidance on responding to access to files and freedom of information requests can also be found on the [Information Commissioner website](#).

The rights of adults at risk, and people alleged to have caused harm including providers are upheld under the [Data Protection Act 1998](#). This means that people have the

- Right of access to personal information held about them

- Right to prevent processing likely to cause damage or distress
- Right to have inaccurate data about them corrected, blocked or erased
- Right to prevent processing of information about themselves for purposes of direct marketing

Applying the data protection principles to the safeguarding principles means that people should be advised at the earliest opportunity of any safeguarding concerns.

[SCIE resource Sharing Information](#) provides guidance for staff on matters of consent and sharing information with family and friends. Additionally intercollegiate guidance is available through Skills for Health recommended link [here](#).

### ***Record Keeping and Professional Accountability***

Every time a record is made of a conversation, observation, telephone call, assessment, professionals should quality assure their own work so it measures up to good information governance:

- Contemporaneous
- Discerns fact from opinion
- Compliant with legislation
- Thorough and relevant
- Contains up to date details

Professionals should be confident that if the service user/provider were to view the record, it would be (a) evidence based (b) written in a professional and respectful manner (c) compliant with relevant legislation. The following questions are a guide:

- What information do staff need to know in order to provide a high quality response?
- What information is needed to keep adults safe?
- What information is not necessary?
- What is the basis for any decision to share (or not) information with a Third Party?

Care should be taken to avoid personal opinion and comments. There is a risk that that this type of recording is seen at a later date as fact which cannot be evidenced. Accuracy is essential, not only for effective safeguarding but ensures resources are not wasted. Using abbreviations is unacceptable unless there is an explanation. Copying of medical notes for example 'R. sided CVA' can waste time and impact on the ability to protect someone. Noting that the person has had a stroke and finds it difficult to talk on the telephone is relevant and provides information that is easily understood by everyone.

A judgement framework needs to consider facts, how different types of evidence can be corroborated and how information can support a reasonable and rational

assessment. Checking with the adult at risk for accuracy is good practice.

Assessments are an on-going process and therefore there is a need to ensure that information is up to date. Ensuring only one record for one person may be part of auditing. Managers might note any concerns where there are duplicate records and implement an immediate action for data cleansing.

When working with Providers, it should be borne in mind that they are reliant upon reputation for their business. Accurate recording that can be backed up by examples and corroborated supports defensible practice.

All records are subject to the retention guidelines set out by the organisation. Through the auditing process records may be disposed of according to each organisations policy. Electronic records should be updated and maintained according to the policy.