

Caldicott Guardian

Warrington Safeguarding Partnership





A Caldicott Guardian is a senior person within a social care organisation who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained.

Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing



There are Caldicott Guardians in:

- Health
- Social Care
- Hospices,
- Clinics,
- Care homes
- Prisons
- GP practices
- Pharmacies
- Charities
- Some providers and commissioners are required by Government to appoint a Caldicott Guardian; others choose to do so because they want to do their best to look after people's information legally and ethically.

The Police have an Information Compliance Team who undertake the same role.

Origin



- Caldicott Guardians derive their name and inspiration from the Government *Review of Patient-Identifiable Information*, chaired by Dame Fiona Caldicott, in December 1997. The review set out six principles for the management of confidential information which support Caldicott Guardians to make balanced judgements for their organisations.
- In 2013 Dame Fiona completed an *Information Governance Review*, which has come to be known as the Caldicott 2 report. It confirmed the enduring relevance of the six principles, but added a seventh:

“the duty to share information can be as important as the duty to protect patient confidentiality.”

Principles - 1



Justify the purpose

- 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.

Principles - 2



Don't use personal confidential data unless it is absolutely 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).



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.

Principles - 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.

Principles - 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.

Principles - 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.

Principles - 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.

Information sharing



This seventh principle was designed to encourage professionals working with children and families to share information across professional or organisational boundaries to maximise safeguarding and quality of intervention.

We have a responsibility to protect and maintain confidentiality, but we must also be aware that safeguarding takes precedence and overrides the duty of confidence.

The Legal bit:



Personal information may be shared legally in one of three ways:

- with the consent of the individual concerned (providing that individual has mental capacity: see Annex C);
- when it is required by law (e.g. The Children's Act 1989 requires information to be shared in safeguarding cases);
- when it is in the public interest.

Relationships



- **Senior Information Risk Owner (SIRO)**
- **Information governance (IG)**

General Data Protection Regulation (GDPR)



Six principles for processing of personal data

The GDPR outlines six data protection principles you must comply with when processing personal data. These principles relate to:

- **Lawfulness, fairness and transparency** - you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** - you must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.
- **Data minimisation** - you must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.
- **Accuracy** - you must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.
- **Storage limitation** - You must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons why you collect this data.
- **Integrity and confidentiality** - You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Questions?

