1997 report of the Review of Patient-Identifiable Information, chaired by Dame Fiona Caldicott followed by the Information Governance Review March 2013 – Fiona Caldicott

Every citizen should feel confident that information about their health is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the health and social care system should see information governance as part of their responsibility.

Our overarching aim has been to ensure that there is an appropriate balance between the protection of the patient or user's information, and the use and sharing of such information to improve care.

It has been gratifying to learn, in the course of the Review, that the Caldicott principles continue to be valuable, but would benefit from minor amendments. The original report was written in 1997 when the service was more paternalistic and much less patient centred. Now citizens are a lot more concerned about what happens to their information; who has access to it, for what purposes is it used, and why isn't it shared more frequently when common sense tells them that it should be.

However, people also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service. So good sharing of information, when sharing is appropriate, is as important as maintaining confidentiality. All organisations providing health or social care services must succeed in both respects if they are not to fail the people that they exist to serve.

The revised list of Caldicott principles therefore reads:

1. Justify the purpose(s)
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.

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).

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.

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.

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.

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.

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.

Strategy & Governance: the Caldicott Guardian should champion confidentiality issues at Board/senior management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

Confidentiality & Data Protection expertise: the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available.

Internal Information Processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

Information Sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS and CSSRs. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related new IT systems, disclosure to research interests and disclosure to the police**.**

Staff should be advised to seek assistance from the Caldicott Guardian where necessary; typical examples of such situations are:

- a request from the police for access to patient information;
- requests from patients to delete their records;
- an actual or alleged breach of confidentiality.

http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott