Introduction

The Caldicott Report was commissioned in December 1997 by the Chief Medical Officer of England owing to increasing concern about the ways in which patient information was used in the NHS in England and Wales and the need to ensure that confidentiality was not undermined.

Such concern was largely due to the development of information technology in the service, and its capacity to disseminate information about patients rapidly and extensively.

One of the recommendations of the report stated that all NHS organisations appoint a Caldicott Guardian to ensure patient-identifiable information is kept secure. (Caldicott Guardians are senior members of staff, preferably at partner level).

Policy Statement

- This document defines the Caldicott Policy for Danetre Medical Practice**.**
- The Caldicott Policy applies to all patient-identifiable information, regardless of whether it is of a medical nature or not, obtained and processed by the Practice.
- This document:
  - Sets out the Practice's policy for the protection of all patient-identifiable information obtained and processed.
  - Establishes the responsibilities for Caldicott Guardianship.
  - Provides reference to the Caldicott principles.

Scope of this Policy

This policy applies to all patient-identifiable information processed, stored on computer or relevant filing systems (manual records) and the Practice staff who use the information in connection with their work.

It also follows the guidelines suggested in the revised version of the GMC document "*Raising and acting on concerns about patient safety*", effective 12 March 2012, a copy of which can be downloaded here:

http://www.gmc-uk.org/Raising_and_acting_on_concerns_about_patient_safety_FINAL.pdf_47223556.pdf

Principles

Patient-identifiable information takes many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.

The Practice will take all necessary steps to safeguard the integrity, confidentiality, and availability of sensitive information.

No staff member employed by the Practice (including temporary or agency staff) is allowed to share any patient-identifiable information unless it has been authorised by the Mgt Team or where appropriate the Practice's Caldicott Guardian.

Dr Amy Butler (Partner) is the Caldicott Guardian at Danetre Medical Practice

It is unlikely that any authorisation to share patient-identifiable data will be granted unless the access is on a need to know basis and justifiable against the Caldicott principles.

The Caldicott standard is based on the following six principles:

- **Justify the purpose(s)** - Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
- **Don't use patient-identifiable information unless it is absolutely necessary** - Patient-identifiable information 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 patient-identifiable information** - Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
- **Access to patient-identifiable information should be on a strict need-to-know basis** - Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- **Everyone with access to patient-identifiable information should be aware of their responsibilities** - Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **Understand and comply with the law** – Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

Training, Policies and Procedures

Danetre Medical Practice takes their responsibilities for the security and protection of all patient-identifiable information very seriously.

All Practice staff have responsibility for compliance with the Caldicott standards. To this end the Practice has:

- Confidentiality clauses in each employee's employment contract;
- Computer based training programmes (including a competency test);
- An Employee Handbook (outlining employee responsibilities);
- Policies, procedures and agreements to ensure any transfer of patient-identifiable information is compliant.

Advice and Guidance

The provision of advice and guidance regarding the Caldicott standard and other relevant legislation may be obtained from **Dr Amy Butler (Partner)** (Head of Information Governance at the Practice).

Validity of this Policy

This policy is in accordance with the Data Protection Act 1998 and its underlying principles.

This policy will be reviewed annually by the Practice's Caldicott Guardian.

Appendix A – Compliance Acts

The Practice adheres to the following Acts:

Data Protection Act 1998 - Data Protection Principles

1. Patient-identifiable data shall be processed fairly and lawfully.

2. Patient-identifiable data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Patient-identifiable data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Patient-identifiable data shall be accurate and, where necessary, kept up to date.

5. Patient-identifiable data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Patient-identifiable data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of patient-identifiable data and against accidental loss or destruction of, or damage to, patient-identifiable data.

8. Patient-identifiable data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of patient-identifiable data.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access.

Each organisation will issue an individual user id and password to each employee which will only be known by that individual and must not be divulged to, or misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities.

Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records 1990

This Act gives patients' representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991.

This Act is only applicable for access to deceased patient's records. All other requests for access to information about living individuals are provided under the access provisions of the Data Protection Act 1998.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Confidentiality: NHS Code of Practice

Gives NHS bodies guidance concerning the required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. It is a key component of information governance arrangements for the NHS.

Appendix B - Caldicott Guardian Role

Danetre Medical Practice has appointed **Dr Amy Butler (Partner)** as its Caldicott Guardian

The Guardian is responsible for the establishment of procedures governing access to, and the use of patient-identifiable information and, where appropriate, the transfer of that information to other bodies.

In addition to the principles developed in the Caldicott Report, the Guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the Protection and Use of Patient Information and on IM&T security disseminated by the Department of Health.

They must also, where necessary, provide advice and support to staff working within the Practice on all aspects of Caldicott, sharing and disclosure of patient-identifiable patient information and related legislation.

Duties and Responsibilities

Production of Procedures, Guidelines and Protocols

- To develop and implement procedures to ensure that all routine uses of patient-identifiable data are identified and documented and that their use has been established as being justified.

- To develop and implement criteria and a process for dealing with ad-hoc requests for patient-identifiable patient data for non-clinical purposes.

- To establish Information Sharing Protocols to govern the use and sharing of patient-identifiable data between organisations both within and outside the NHS.

- To ensure standard procedures and protocols are in place to govern access to patient-identifiable data.

Staff Information

- To ensure standard procedures and protocols are in an understandable format and available to all staff
- Raise awareness through training and education to ensure that the standards of good practice and Caldicott principles are understood and adhered to.

- Advise project leads on all aspects of Caldicott, acting as an expert resource for them.

Reporting

- To bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed.

- To raise concerns about any inappropriate uses of patient-identifiable data with external bodies where necessary.

- On an annual basis, to participate in the Information Governance Toolkit Assessment

Additional Notes

- The duties and responsibilities outlined above are to be regarded as broad areas of responsibility and do not necessarily detail all tasks which the post holder may be required to perform.

- This job description may be subject to change in the light of experience and circumstances and after discussion with the post holder.

- The post holder will be expected to act with full regard to the requirements of the Practice's policies and procedures, including those relating to Health and Safety.

- The Caldicott Guardian will be expected to liaise and work with external bodies in the course of promoting the Caldicott principles, which may include attendance at various meetings as appropriate.