# Policy Name: Caldicott Protocol

## Policy Number: 60

**Background**

The principle of Caldicott Guardianship was established in 1997 following the publication of the Caldicott Report from the review chaired by Dame Fiona Caldicott. The review was commissioned by the Chief Medical Officer because of increasing concerns about how patient information was being used in the NHS, specifically the way in which it was being stored and transferred electronically.

The report made 16 recommendations regarding the safeguarding of patient-identifiable information, including the requirement for NHS organisations to appoint a Caldicott Guardian. It also established the six Caldicott principles, which should be considered before any disclosure of patient identifiable information in order to protect patient confidentiality:

A later review revisited the Caldicott principles, which remained the same except that they no longer refer to “patient identifiable information” but “personal confidential data”. More importantly however, the review introduced a new eigth principle.

1. Justify the **purpose**(s)
2. Only use it when absolutely **necessary**
3. Use the **minimum** amount of patient-identifiable information necessary to perform the task
4. Access to patient-identifiable information should be on a strict “**need-to-know**” basis
5. Everyone must understand their **responsibilities**
6. Everyone should understand and comply with the **law**
7. The duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is used

**The Caldicott Guardian/Information Governance Lead**

Andrea Trafford, Business Manager is the Caldicott Guardian/Information Governance Lead for The Chorley Surgery, with Dr Magapu as the clinical lead.

Michelle Brisco is Deputy Lead for Information Governance.

**Responsibilities**

* Strategy and Governance – strategic overview and representation.
* Confidentiality and data protection – knowledge of confidentiality and data protection.
* Internal Information Processing – practice procedure and policy compliance.
* Information Sharing – information provided externally to be assessed, controlled and compliant.

**The Caldicott Principles:**

1. ***Justify purpose***

Every proposed use or transfer of patient-identifiable information within or from the practice should be clearly defined or scrutinised. Continued use of information should be subject to regular review by the Information Governance Lead.

1. ***Only Use When Necessary***

Where it is not necessary to identify the patient within a flow of information, then this identifying information should be excluded. The need for the identification of a patient should be considered at each stage of a process, and this information should not be provided unless there is no alternative.

1. ***Use the Minimum Necessary***

Where identifying information is essential, only use the minimum amount to enable the patient to be identified positively, e.g. use of unique patient number combined with date of birth may be sufficient to identify the patient without the possibility of error, negating the need to use names and addresses. Where the use of identifiable information is considered essential, then each individual item of information within the data set should be justified with the aim of reducing identifiability, and therefore the resultant risk should the information be illegally accessed.

1. ***Access on a Need to Know Basis***

Only persons who need to have the information should have access, and then only to the parts of the record which they need. This may involve access control, the split of access rights, or the split of processes or information flows to ensure that this can be achieved. IG Leads will be responsible for the agreement and the review of internal patient flows and protocols to ensure that patient identifiable information is protected.

1. ***Awareness of Responsibilities***

All staff should receive annual training and regular awareness briefings, with suitable clauses in policy documents and contracts of employment. Both clinical and non-clinical staff should to be aware of the practical application of the requirements in patient-facing situations.

1. ***Comply with the Law***

The IG Lead within the practice should maintain a knowledge of relevant legislation (see above) commensurate with their role and level of responsibility. The IG Lead should be responsible for compliance with legal requirements.

1. **The Duty to Share Information**

Staff should be confident that they can share information when it is in the best interests of patients and within the framework of the Caldicott Principles.

1. **Inform patients and service users about how their confidential information is used**

Steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this

**Caldicott Review 2**

In 2012, Dame Fiona Caldicott was asked to lead a second piece of work - this time because of concerns regarding the balance **- or rather the imbalance -** between the protection of patient information and the use and sharing of information to improve patient care. Basically, there was a growing concern that IG was being used as an excuse for not sharing information, even when it would have been in the patient’s best interests.

**Announcement of new Caldicott Principle – December 2020**

The National Data Guardian for Health and Social Care (NDG) Dame Fiona Caldicott published the [outcomes from a public consultation](https://www.gov.uk/government/consultations/caldicott-principles-a-consultation-about-revising-expanding-and-upholding-the-principles) that she ran to seek views on her intention to revise the existing 7 Caldicott Principles. The new principle’s purpose being to make clear that patients and service user expectations must be considered and informed when confidential information is used, to ensure no surprises about the handling or sharing of their data.

The resulting report (Information: to Share or not to Share? The Information Governance Review, March 2013) commonly known as the Caldicott2 report, makes 26 recommendations. **The key message from the report is that all organisations providing health and social care services must succeed in maintaining confidentiality and information governance standards, but also practice good sharing of information when this is appropriate.**

The report also recommends that regulatory, professional and educational bodies should ensure that sound record keeping **and the importance of data quality,** are part of continuous professional development and assessed as part of the professional revalidation process.

All of the 26 recommendations were accepted by the Government in their response to the review and Dame Fiona has been tasked with publishing another report one year later on progress made on implementing these across Health and Social Care.

**Caldicott Audit**

A tool for auditing the practice’s compliance with Caldicott is provided as **Appendix A**.

**Practice Staff Guidance**

Members of staff have a responsibility to ensure security of patient data, which may be held in various forms such as computer-held records, paper files, videos etc. On a day-to-day basis the Caldicott principles will apply mainly to patient-identifiable data held within paper-based medical records or on a patient-based clinical system.

**Basic principles of information handling within the Practice are:**

* Patients should be informed how their data is used
* Patients should be informed who will have access to their data, and when/why
* There should be an understanding of data which may only be released with express consent
* Staff should be aware of patients’ rights to access their record, and to discuss / correct errors
* Patients who wish to have their information withheld for a specific purpose should have their rights respected unless there are special circumstances – statutory matters, court orders, public health issues etc.
* Where disclosure is to take place regardless of patient consent, there should be an attempt to agree or discuss the issues with the patient first
* Access to patient information must be strictly on a health-needs basis, and staff should only access patient records when it is required to perform business tasks
* Records must remain secure and confidential at all times. Access to records on computer systems should be password protected, and staff should not leave their terminal whilst still logged on
* Contracts of employment, staff handbooks, visitor agreements, and sub-contractor agreements will contain a specific confidentiality clause

**Access Controls**

* **Manual records**
* To be held in a lockable area
* Storeroom door kept closed and notes not left in consulting or general office areas
* Filing cabinets locked. Rooms locked outside normal surgery hours
* Reception cover always in place to prevent non-staff access to secure areas
* Records only removed from the practice for specific purposes (e.g. home visits) and returned same day (not held off-site overnight)
* **Computerised Records**
* Differential access rights in force related to role
* Full audit trail facilities
* Access levels controlled by operational managers
* Automatic password change prompts on all systems
* New starters and leavers to have immediate access status updates
* Active screen savers cut in at short delay intervals
* Consulting room screens cleared of last patient detail prior to calling next patient in
* Automatic log-out of systems when unused for short time period
* Full back-up and storage protocols in place

**Sharing of Information**

* All external information flows documented and retained securely
* All confidentiality agreements documented and retained securely
* No confidential information passed to third parties without express consent (where appropriate)
* Community staff have access, subject to agreement, commensurate with their role

**General**

* Visitor log on TEAMNET maintained
* Confidential conversations conducted relative to the security of the environment
* Original medical records not released to third parties
* Emailing of patient data restricted to NHS.NET/secure network

**Policies / Protocols**

The Chorley Surgery has the following policies in place which support the Caldicott Principles:

* Access to Medical Records – Policy No.1
* Clinical Governance Policy – Policy No. 64
* Computer and Data Security Policy – Policy No. 102
* Computer, Internet and Email Policy – Policy No. 105
* Confidentiality Policies/Agreements (various)
* General Data Protection Regulations Policy – Policy No.8
* Disclosure / Sharing of Patient Information Policy– Policy No. 30
* Electronic Transfer of Patient Data policy – Policy No. 103
* Freedom of Information Act Policy – Policy No.11
* Practice Security Procedures – Policy No. 108
* I.G Risk Management (Toolkit) – Policy No. 55

Since the original Caldicott report was published in 1997, a number of other statutory regulations have added to and enhanced the principles of Caldicott. Some examples of these include:

* Human Rights Act 1998
* Data Protection Act 2018
* Freedom of Information Act 2000
* Equality Act 2010

And other guidelines have been published such as:

* NHS Code of Practice on Confidentiality (2003)
* The NHS Constitution for England
* The Care Records Guarantee
* A Guide to Confidentiality in Health and Social Care, HSCIC
* Code of Practice on Confidential Information (draft out for consultation) HSCIC
* The Caldicott Guidance Manual 2010
* IG Toolkit requirements
* Information: to Share or not to Share? The Information Governance Review, April 2013
* Information: to Share or not to Share, Government Response to the Calidcott Review, Sept 2013

**Appendix A – The Chorley Surgery Caldicott Audit model**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Item*** | ***Unsatisfactory*** | ***Acceptable but could be improved*** | ***Satisfactory*** |
| Information provided to patients on the use of their information | No information provided or limited to simple posters and leaflets in the waiting room | An active information campaign in place to promote understanding of NHS information requirements | An active information campaign supported by comprehensive arrangements for patients with special / different needs |
| Staff Code of Conduct for Confidentiality | No code exists, or staff not generally aware of it | Code of Conduct exists and staff are aware of it | Code regularly reviewed and updated as required |
| Staff Induction procedures | No mention of Confidentiality and security requirements in induction for most staff | Basic requirements outlined as part of the induction process | Comprehensive awareness undertaken and comprehension checked |
| Confidentiality and Security training needs | Training needs not assessed systematically for most staff | Training needs only assessed as a consequence of systems changes | Systematic assessment of staff training needs and evaluation of training that has occurred |
| Training Provisions (confidentiality and security) | No training available to the majority of staff | Training opportunity broadcast with take-up left to managers discretion | In house training provided for staff |
| Staff Contracts | No reference to confidentiality requirements in contracts | Confidentiality included in some staff contracts | Confidentiality included in all staff contracts |
| Contracts with other organisations | No confidentiality requirements included | Basic agreements of undertaking signed by contractors | Formal contractual arrangements exist with all contractors and support organisations |
| Protocols for sharing information with other local organisations agreed | No locally agreed protocols in place | Partner organisations clearly identified and information requirements understood | Agreed protocols in place to govern the sharing and use of confidential information |
| Security responsibility | No information security officer, or existing officer not fully trained | An appropriately trained information security officer is in place | Responsibility for information security identified in a variety of staff roles and is coordinated by the IG Lead/Caldicott Guardian |
| Security incidents | No incident control or investigation procedures | The security officer handles incidents as they occur | Procedures are documented and accessible to staff to ensure incidents are investigated promptly |
| User responsibilities | No guidance to staff on password management | Users encouraged to change passwords regularly at their discretion | Password changes enforced on a regular basis |
| Controlling access to confidential patient information | Staff vigilance or “honour” system to control access. Some physical controls | Access for many staff on an “all or nothing” basis. Staff group access agreed with IG Lead/Caldicott Guardian | All staff have defined, documented access rights agreed by the IG Lead/Caldicott Guardian. Access controlled monitored and audited |