REVIEW

What is a Caldicott guardian?

C Roch-Berry

Postgrad Med J 2003;**79**:516–518

A review of patient confidentiality issues was commissioned and its findings published as the *Caldicott Report* in December 1997. It made 16 recommendations and formulated six principals. To help in remembering these principles the mnemonic FIONA C can be used: **F**ormal justification of purpose; **I**nformation transferred only when absolutely necessary; **O**nly the minimum required; **N**eed to know access controls; **A**ll to understand their responsibilities; **C**omply with and understand the law. Since the *Caldicott Report* in 1997 the following acts have become law. Data Protection Act 1998, Human Rights Act 1998, Public Interest Disclosure Act 1998, Audit Commission Act 1998, Terrorism Act 2000, section 60 of the Health and Social Care Act 2001 and Regulation of Investigatory Powers Act 2000, and by 2005 The Freedom of Information Act 2000 will become law and affect the NHS. Consequently it can be seen that the role and responsibility of Caldicott guardians has grown significantly into what is now known as information governance.

Correspondence to:
Dr Colin Roch-Berry, Cheltenham General Hospital, Sandford Road, Cheltenham GL53 7AN, UK; Colin.Roch-Berry@egnhst.org.uk

Submitted 2 August 2002
Accepted
14 January 2003

The *Caldicott Report* was published in 1997 and made recommendations relating to patient confidentiality. The position of Caldicott guardian was set up in response to this report and this review describes the background and their role and responsibilities.

WHAT IS A CALDICOTT GUARDIAN?

A review was commissioned by the Chief Medical Officer of England owing to increasing concern about the ways in which patient information is used in the NHS in England and Wales and the need to ensure that confidentiality is 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. In 1996 guidance on "the protection and use of patient information" was promulgated and there was a need to promote awareness of it at all levels in the NHS. It did not affect Scotland originally but they have recently adopted it.

A main committee was set up under the Chair of Dame Fiona Caldicott and there were four separate working groups. Dame Fiona Caldicott was Principal of Somerville College, Oxford and consultant psychiatrist and Past President of the Royal College of Psychiatrists. Needless to say the committee was known as the Caldicott Committee. The Caldicott Committee terms of reference was to review all patient-identifiable information, which passes from NHS organisations to other NHS or non-NHS bodies for purposes other than direct care, medical research, or where there is a statutory requirement for information. The committee was to consider each flow of patient-identifiable information and was to advise the NHS Executive whether patient identification was justified by the purpose and whether action to minimise risks of breach of confidentiality was desirable—for example, reduction, elimination, or separate storage of items of information. Some 86 flows of patient-identifiable information were mapped relating to a wide range of planning, operational, or monitoring purposes. Within the context of current policy, all of the flows identified were for justifiable purposes. The Caldicott Report was published in December 1997.

The Caldicott Committee made a total of 16 recommendations, namely:

- *Recommendation 1:* Every dataflow, current or proposed, should be tested against basis principles of good practice. Continuing flows should be retested regularly.
- *Recommendation 2:* A programme of work should be established to reinforce awareness of confidentiality and information security requirements among all staff within the NHS.
- *Recommendation 3:* A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.
- *Recommendation 4:* Clear guidance should be provided for those individuals/bodes responsible for approving uses of patient-identifiable information.
- *Recommendation 5:* Protocols should be developed to protect the exchange of patient-identifiable information between NHS and non-NHS bodies.
- *Recommendation 6:* The identity of those responsible for monitoring the sharing and transfer of information within agreed local protocols should be clearly communicated.
- *Recommendation 7:* An accreditation system which recognises those organisations following good practice with respect to confidentiality should be considered.
- *Recommendation 8:* The NHS number should replace other identifiers wherever practicable, taking account of the consequences of errors and particular requirements for other specific identifiers.

- *Recommendation 9:* Strict protocols should define who is authorised to gain access to patient identity where the NHS number or other coded identifier is used.
- *Recommendation 10:* Where particularly sensitive information is transferred, privacy enhancing technologies (for example, encrypting identifiers or "patient-identifying information") must be explored.
- *Recommendation 11*: Those involved in developing health information systems should ensure that best practice principles are incorporated during the design stage.
- *Recommendation 12:* Where practicable, the internal structure and administration of databases holding patient-identifiable information should reflect the principles developed in this report.
- *Recommendation 13:* The NHS number should replace the patient's name on items of service claims made by general practitioners as soon as practically possible.
- *Recommendation 14:* The design of new systems for the transfer of prescription data should incorporate the principles developed in this report.
- *Recommendation 15:* Future negotiations on pay and conditions for general practitioners should, where possible, avoid systems of payment, which require patient-identifying details to be transmitted.
- *Recommendation 16:* Consideration should be given to procedures for general practice claims and payments, which do not require patient-identifying information to be transferred, which can then be piloted.

The Caldicott Committee also formulated six principles, namely:

- *Principle 1—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.
- *Principle 2—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).
- *Principle 3—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.
- *Principle 4—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.
- *Principle 5—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.
- *Principle 6—Understand and comply with the law:* Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient-identifiable information should be responsible for ensuring that the organisation complies with legal requirements.

Box 1: Questions (answers at end of paper)

1. When was the report commissioned?
2. How many recommendations did it make?
3. What are the six principals?
4. How often is the 18 point management audit to be carried out?
5. Name three information/confidentiality acts passed since the *Caldicott Report*?
6. Will the Freedom of Information Act affect the NHS?

To help in remembering these principles the mnemonic FIONA C can be used:

- **F**ormal justification of purpose
- **I**nformation transferred only when absolutely necessary
- **O**nly the minimum required
- **N**eed to know access controls
- **A**ll to understand their responsibilities
- **C**omply with and understand the law

Caldicott guardians were supplied with an 18 point management audit tool (see table 1) to be used at set up and then annually. Results were to be presented to the trust board and returned to the Department of Health. The report also details where improvements can be made in the in the ensuing year and priority of action.

There is a national audit list of NHS trusts, primary care trusts, etc with each audit profile being awarded 0, 1, or 2 points. It is anticipated that in the future there will be some outside assessor looking at the accuracy of each trusts own assessment. Since the *Caldicott Report* was published in December 1997 the law concerning confidentiality and consent has been strengthened. A new Data Protection Act was passed in 1998, which embraced paper records as well as computerised records. The European Convention of Human Rights was incorporated into English law by the Human Rights Act 1998. Disclosure of confidential information without consent in particular situations is covered by Public Interest Disclosure Act 1998, Audit Commission Act 1998, Terrorism Act 2000 and section 60 of the Health and Social Care Act 2001. The responsibilities of Caldicott guardian have been extended by the Regulation of Investigatory Powers Act 2000 and by 2005 The Freedom of Information Act 2000 will affect the NHS. Consequently it can be seen that the role and responsibility of Caldicott guardians has grown into what is now known as information governance.

The Caldicott guardian is available to give advice to individuals in the trust, to the ethics committee, and departments. The guardian also writes trust policies concerning confidentiality in its broadest sense. Many staff are not aware of confidentiality problems particularly in giving information to the patient's extended family. Many doctors find it difficult to realise that although they can access their patient's health records, this may only be done in the context of medical care and not for research purposes. Casualty staff in particular find the police daunting and need advice as to what information the police have a right to know. The Caldicott guardian has to access confidential files when information is to be revealed under the Data Protection Act especially when the consultant in charge of the case is dead or retired to make sure there is no breach of duty in giving third party information etc. In most general cases, for example in cancer registries or cancer waiting times, a block judgment has to be made.

The trust has a comprehensive monitoring system and breaches of confidentiality are notified to the Caldicott guardian and data protection officer. The actual investigation is

Table 1 The management audit organisational profile

	Title	Level 0	Level 1	LeveL 2
1.	Information for patients/clients on the proposed uses of information about them	No information provided, or limited to simple posters and leaflets in waiting rooms	An active information campaign is in place to promote patient understanding of NHS information requirements	An active information campaign is supported by comprehensive arrangements for patients with special/different needs
2.	Staff code of conduct in respect of confidentiality	No code exists, or staff not generally aware of it	Code of conduct exists and all staff aware of it	Code regularly reviewed and updated as required
3.	Staff induction procedures	No mention of confidentiality and security requirements in induction for most staff	Basic requirements outlined as part of induction process	Comprehensive awareness raising exercise undertaken and comprehension checked
4.	Confidentiality and security Training needs assessment	Training needs not assessed systematically for most staff	Training needs only considered as a consequence of organisational or systems changes	Systematic assessment of staff training needs and evaluation of training that has occurred
5.	Training provisions (confidentiality and security)	No training available to the majority of staff	Training opportunities broadcast with take up left to line management discretion	In-house training provided for staff—for example compatible to health and safety training provision
6.	Staff contracts	No reference to confidentiality requirements in staff contracts	Confidentiality requirements included in contracts for some staff	Confidentiality requirements included in all staff contracts
7.	Contracts placed with other organisations	No confidentiality requirements included	Basic agreements of undertaking are signed by contractors	Formal contractual arrangements exist with all contractors and support organisations
8.	Reviewing information flows containing patient-identifiable information	Information flows have not been comprehensively mapped	Information flows have been mapped and senior management has been informed	Procedures are in place to regularly review information flows and justify purposes
9.	Internal information/data "ownership" established	Information flows have not been comprehensively mapped	"Ownership" established for all information/data sets and register established	All "owners" justifying purposes and agreeing staff access restrictions with the guardian
10.	Safe Haven procedures in place to safeguard information flowing to and from the organisation	No Safe Haven procedures used	Safe Haven procedures used for some information flows	Safe Haven procedures in place for all patient-identifiable information
11.	Protocols governing the sharing of patient-identifiable information with other organisations locally 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
12.	Security policy document	No security policy available	Security policy exists but not reviewed within the last 12 months	Security policy reviewed annually and reissued if appropriate
13.	Security responsibilities	No information security officer appointed, or existing officer is not appropriately trained	An appropriately trained information security officer is in post	Responsibility for information security identified in various staff roles, coordinated by security officer
14.	Risk assessment and management	No programme of information risk management exists	A risk management programme is underway and reports are available	A formal programme exists with regular reviews, outcome reports, and recommendations provided for senior management
15.	Security incidents	No incident control or investigation procedures exist	The security officer handles incidents as they arise	Procedures are documented and accessible to staff to ensure incidents reported and investigated promptly
16.	Security monitoring	No monitoring or reporting of security effectiveness or incidents takes place	Basic reporting of major incidents or problem areas only	There are regular reports made to senior management on the effectiveness of information security
17.	User responsibilities	No guidance issued to staff for password management	Users encouraged to change passwords regularly but this is at their discretion	Password changes are enforced on a regular basis
18.	Controlling access to confidential patient information	Staff vigilance, and/or an "honour" system control access. Some physical controls, lockable rooms etc may exist	Access for many staff controlled by "all or nothing" systems. Staff groups requiring access identified and agreed with the guardian	All staff have defined and documented access rights agreed by the guardian. Access is controlled, monitored, and audited

carried out by the line manager or in the case of senior managers by the head of human resources. As the role of the Caldicott guardian has expanded the time needed has increased. The author allocates six sessions per week to his Caldicott duties. With this growing responsibility it is very important that the Caldicott guardian has a comprehensive backup. Consequently the author chairs an information governance group which comprises of the director of information, director of operations, head of human resources, head of it services, clinical information manager, IM&T manager, risk manager, legal claims manager, data protection coordinator, EPR clinical lead, assistant facilities manager, Caldicott implementation project manager, IHCS manager, and the communications manager. It meets for two hours every two months. It is a coordinating group, which monitors trust-wide security matters in its broadest sense and reports to the trust board and to the necessary heads of department if there appears to be problems.

BIOGRAPHICAL NOTE

The author was appointed Consultant Clinical Oncologist in Cheltenham in 1975 and took partial retirement in 1999 to become a Caldicott guardian. Apart from his medical background he graduated LLM from Cardiff University in 1991, the degree being in legal aspects of medical practice.

ANSWERS

1. December 1997; 2. 16; 3. Formal justification of purpose, information transferred only when absolutely necessary, only the minimum required, need to know access controls, all to understand their responsibilities, comply with and understand the law; 4. Annually; 5. Data Protection Act, Human Rights Act, Public Interest Disclosure Act, Audit Commission Act, Terrorism Act 2000 and section 60 of the Health and Social Care Act 2001; 6. Yes. Trusts etc are public bodies as defined by the Act.