The Caldicott report

The Caldicott report and patient confidentiality

M A Crook

An introduction for the pathologist

In 1997, the Caldicott committee presented its report on patient confidentiality.[1] The impetus behind this were concerns about patient information and security.[2 3] For example, there had been reports in the press that patient hospital records could be freely accessed and that patient notes had ended up lying around in village streets for all and sundry to read.

The committee came up with six main principles as follows.

(1) One should justify the purpose of holding patient information.

(2) Information on patients should only be held if absolutely necessary.

(3) Use only the minimum of information that is required.

(4) Information access should be on a strict need to know basis.

(5) Everyone in the organisation should be aware of their responsibilities.

(6) The organisation should understand and comply with the law.

National Health Service (NHS) organisations should have Caldicott guardians who have responsibilities to safeguard and govern the use of patient information. The guardian is usually a board level health professional or their deputy. They should develop local protocols for information disclosure, restrict access to patient information by enforcing strict need to know principles, and regularly review and justify the uses of patient information.

Recommendation 1. Every dataflow, current or proposed, should be tested against basic principles of good practice. Continuing flows should be tested regularly

Recommendation 2. A programme of work should be established to reinforce awareness of confidentiality and information security requirements among staff within the National Health Service (NHS)

Recommendation 3. A senior person, preferably a health care professional, should be nominated in each health organisation to act as guardian, responsible for safeguarding the confidentiality of patient information

Recommendation 4. Clear guidance should be provided for those individuals/bodies 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 local protocols should be clearly communicated

Recommendation 7. An accreditation system that 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 identities

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 (such as encrypting identifiers or patient identifying information) must be explored

Recommendation 11. Those involved in developing health information systems should ensure that the best practice principles are incorporated during design stage

Recommendation 12. Where practicable the internal structure and administration of databases holding patient identifiable information should reflect the principles developed inthis 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 that require patient identifying details to be transmitted

Recommendation 16. Consideration should be given to procedures for general practice claims and payments that do not require identifying information to be transferred, which can then be piloted

Figure 1 Recommendations of the Caldicott committee to ensure patient confidentiality.

(1) The personal data shall be held and used lawfully
(2) There must be a clear reason for holding the information and it should be used only for that purpose
(3) The information should not be superfluous but sufficient for the purpose
(4) The information should be up to date and accurate
(5) The information should not be held longer than is necessary
(6) The individual's rights must be upheld with respect to their information
(7) Suitable security should be in place to protect data
(8) Information should not be transferred to or accessed from a country outside the European economic area unless adequate data protection systems are guarenteed

Figure 2 The eight main principles of the Data Protection Act.

The Caldicott committee also came up with recommendations for ensuring patient confidentiality, which are summarised in fig 1.

> "National Health Service organisations should have Caldicott guardians who have responsibilities to safeguard and govern the use of patient information"

These principles regarding patient confidentiality are also entrenched in the NHS core plan. Indeed, the NHS plan core principle 10 states that "patient confidentiality will be respected throughout the process of care". The Data Protection Act 1998 is also relevant in this context. The aim of this act is to uphold an individual's right to privacy with regard to the processing of personal data. There are eight main principles of this act (fig 2).

Where does this lead us as pathologists? First, I suspect that patient confidentiality will feature more and more within the NHS with the associated potential for litigation. Caldicott issues will probably be used as NHS performance indicators based partly upon the Caldicott audit returns. For example, we will need to ensure secure transmission and distribution of our patients' data, such as accurate faxing of laboratory results to information safe havens, and use password protected computer systems. Information technology security should comply with BS7799 and the Data Protection Act. In addition, we should take particular care of the safety of patient notes and ensure patient consent where necessary regarding confidentiality issues. The only time that patient information can be divulged to a third party is if the patient has given their properly informed consent for this to happen, or if the data are totally anonymised to prevent identification of the patient from the details given.

The General Medical Council statement on confidentiality (September 2000) also remarked that as doctors we hold information about patients, which is private and sensitive. This information must not be given to others

unless the patient consents or the disclosure can be justified. We will also need to establish training programmes about patient confidentiality for our staff and help map patient information flows, to name but a few areas. Non-consensual data sharing may be deemed contrary to medical ethics and where possible anonymised patient data should be used.[4–7]

These aspects of patient confidentiality are summarised as the Caldicott audit points shown in table 1.

Section 60 of the Health and Social Care Act, passed by parliament in May 2001, gives the secretary of state for health the power to allow the processing of patient information for medical purposes if these purposes are in the public interest (for example, cancer registries). "Patient information" in this context means any health or medical information about the patient, whether identifiable with an individual or not. The government also agreed to the establishment of a statutory advisory committee (the patient information advisory group) to keep the provisions on confidential data and their use by the secretary of state under review.

In summary, patient information and confidentiality issues will probably gain increasing importance in the following years within the NHS. A balance between individual data privacy and useful information exchange for the benefit of society will need to be struck.[8] On that note, do not forget the Caldicott principles' mnemonic, a reminder of Dame Fiona Caldicott herself:

Table 1 Caldicott audit points

Audit points		Audit level 0	Audit level 1	Audit 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, etc	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 provision (confidentiality and security)	No training available to most staff	Training opportunities broadcast with take up left to line management discretion	In house training provided for staff; for example, comparable 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	Contractual 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 for the regular review of information flows and the justification of purposes
9	Internal information/data "ownership" established	Information/data "ownership" has not been established for all information/data sets	"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 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 the security officer
14	Risk assessment and management	No programme of information risk management exists	A risk management programme is under way 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

FIONA C

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.

This may help us to focus on patient confidentiality in our clinical work; remembering it to be an important part of risk management and clinical governance.

J Clin Pathol 2003;**56**:426–428

Correspondence to: Dr M A Crook, Guy's, St Thomas's, and University Hospital Lewisham, London SE13 6LH, UK; martin.crook@uhl.nhs.uk

REFERENCES

1 **The Caldicott report**. *IHRIM* 1999;**40**:17–19.
2 **Wiederhold G**. Future of security and privacy in medical information. *Stud Health Technol Inform* 2002;**80**:213–29.
3 **Gaunt N**. Practical approaches to creating a security culture. *Int J Med Inf* 2000;**60**:151–7.
4 **Data Protection Act**, 1998.
5 **Access to health records**, 1990.
6 **Computer Misuse Act**, 1990.
7 **Human Rights Act**, 1998.
8 **Anderson R**. Undermining data privacy in health information. *BMJ* 2001;**322**:442–3.