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. The impetus behind this was concerns about patient information and security. 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.

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

The Caldicott report and patient confidentiality

M A Crook

An introduction for the pathologist

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

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.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.6 On that note, do not forget the Caldicott principles’ mnemonic, a reminder of Dame Fiona Caldicott herself:

Table 1 Caldicott audit points

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

REFERENCES