Patient confidentiality: where are we now?

Every day the NHS collects a lot of information relating to individual patients. This information is not gathered solely for the effective management of patients' clinical conditions, but also for many other purposes such as planning services, agreeing the amount of services provided at local hospitals and public health. With the advent of modern technology, increasingly data are transferred electronically and with the rapid development of electronic patient records, the amount of information stored and shared electronically will increase and with it the potential for breach of security and confidentiality. A lot of attention has been given to this issue nationally.

NATIONAL CONTEXT

Regulatory bodies have always been concerned with confidentiality issues, as a duty to support professional ethical standards; the General Medical Council (GMC) for example produced comprehensive guidance to doctors on confidentiality (GMC, 2000). In this it enlarges on the principles listed in *Good Medical Practice* (GMC, 1998) and reminds professionals of their duty to respect the patient's rights not to have their personal details disclosed. This guidance makes it clear that such disclosure requires the patient's consent and that patients must be informed when any information is likely to be disclosed to others involved in their care, so that they have the opportunity to withhold permission; and gives guidance about responsibility of doctors within their team. It also covers education and research.

The guidance, *The Protection and Use of Patient Information* (NHS Executive, 1996), states that when patient information is used, it should be anonymized and that only the minimum required should be shared. The Chief Medical Officer then set up a committee to review all transfer of patient-identifiable information within the NHS and between the NHS and non-NHS bodies for purposes other than direct care. In its report (Department of Health, 1997) the Caldicott Committee stressed the importance of preventing unnecessary identification of individual patients, the importance of using the NHS number and the need to strengthen internal processes so that information used for non-clinical purposes does not allow the identification of individual patients. It also listed a set of principles to bear in mind when sharing patient information (*Table 1*) and recommended the establishment of a network of Caldicott Guardians responsible for agreeing and reviewing the organization's protocols governing the transfer and disclosure of patient identifiable information and for developing security and confidentiality policies.

The publication of the Caldicott report was followed by a number of circulars dealing with its implementation; all NHS organizations had to appoint a Caldicott Guardian, preferably a clinical member of the trust board. This responsibility therefore fell upon either the medical or the nursing director (usually the director taking the lead for clinical governance). Organizations also had to undertake an audit of current practices in order to identify what needed to be done over time and put together an action plan with clear timescale.

For the Record, a health service circular published in 1999, reminds individuals handling records or coming across patient information that they have 'a personal common law duty of confidence to patients and to his or her employer' (NHS Executive, 1999); this duty prohibits the use and disclosure of patient information without consent, unless it is statutorily required. The need for research using patient-identifiable information to get approval from ethics committee is also reinforced. Patients can therefore have some control over who is able to access the information they have given to healthcare professionals.

With the implementation of the NHS plan and the information strategy underpinning it, the issue of security and confidentiality is becoming even more important. A strategy for confidentiality building on the work of the Caldicott report is thus needed and is being developed by the Information Policy Unit of the Department of Health (Thorp and Walker, 2001). Moreover the Caldicott standard is being implemented in social care as a foundation for good joint working (Department of Health, 2002) and as such Caldicott Guardians will also be established within councils with social services responsibilities. There are many other important guides dealing with security and confidentiality which can be found on the Department of Health website (www.doh.gov.uk) and the Information Policy Unit website (www.doh.gov.uk/ipu); the latter has a section dedicated to patient confiden-

TABLE 1.
Caldicott principles

1. Justify the purpose(s) for which information is required
2. Do not use patient-identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient-identifiable information
4. Access to such information should be on a strict need-to-know basis
5. Everyone with access should be aware of their responsibilities
6. Understand and comply with the law

tiality. The legal requirements are covered by the Data Protection Act 1998, which covers manual and electronic records, and the Computer Misuse Act 1990, which provides sanctions against unauthorized access.

LOCAL ACTION

Maintaining the confidentiality and security of patient information is fundamental to the relationship between patients and health-care professionals and is an integral part of the ethics of the professions. Patients need to understand that clinical information may be used for purposes other than their clinical management and that this information may be passed to agencies involved in their care planning, such as social services. As such health-care organizations need to ensure that proper processes and protocols are in place to safeguard this information; this also applies to the social care sector since they are in the process of implementing the Caldicott standard. So what do these organizations need to do?

They should have written notices explaining how information is used, what rights patients have and how confidentiality will be respected. This should give contact details where concerns can be raised and queries answered. An explicit procedure for patients' access to their own record must be in place to avoid delay, giving details including contact person and checks required. Each employee must be made aware of their responsibilities and reminded that they have to comply with the law. All staff should sign a confidentiality agreement and confidentiality, security and ethical issues should form part of the induction programme of new staff. Training should be provided for staff, including junior doctors, so that they understand the legal requirements and the meaning of the duty of confidence.

The Caldicott Guardian, on behalf of the organization, needs to oversee the implementation of the Caldicott improvement plan and ensure that the relevant processes for vetting information flow and approving protocols for transfer of information between agencies are in place and reviewed regularly. The Caldicott principles should form the standards against which these flows and protocols are tested, so that identifiable data are not released inappropriately.

Staff also need to be aware of their responsibility to maintain confidentiality at all times. Clinical staff need to make sure that when discussing patient's conditions with colleagues or clinical problems with the patients, others do not overhear them, an issue to be borne in mind when doing ward rounds. They also need to make sure the information given to them is effectively protected against improper disclosure, such as ensuring that written medical records are not left unattended in 'public' places and are properly secured. They need to respect patients' requests for confidentiality, and on occasion this may conflict with the request of the relatives. They must never disclose information gathered in the course of their work to a third party and must be prepared to explain and justify a decision to release confidential information. Furthermore, they need to comply with the law at all times and accept the consequences when a breach occurs. There are occasions when it is in the public interest to share information, but staff should not do so without taking advice from the Caldicott Guardian, to ensure that their action is not breaking the law.

CONCLUSION

Good communication between professionals within the NHS and in other agencies is necessary if patients are to be managed effectively. This requires information about individual patients to be shared and increasingly this information is going to be transferred electronically; security and confidentiality must be safeguarded at all times. While policies are being developed at a national level, it is at a local level that the right processes and protocols need to be in place to make this a reality. Training for staff needs to be available so that patients can remain confident that personal information is safe in the hands of their local health services. HM

KEY POINTS

- Trust between patients and health-care professionals requires assurance that confidentiality will be maintained at all times.
- Staff have a personal common law duty of confidence to patients and must comply with their professional ethical standards.
- Patient/client information should not be disclosed without consent.
- Organizations need to ensure that appropriate processes and protocols are in place to safeguard patient/client information.
- Organizations need to ensure that staff are familiar with the Data Protection Act 1998, the Computer Misuse Act 1990 and any other requirements with regards to confidentiality.
- Patients need to know who to contact if they have concerns about confidentiality issues.
- Increasing attention needs to be given to confidentiality and security of patient-identifiable data as more information is transferred electronically and electronic patient records are implemented.

Myriam Lugon
Consultant Clinical Governance and Healthcare Policy
c/o Royal Society of Medicine Press Limited
1 Wimpole Street
London W1G 0AE

Department of Health (1997) *The Caldicott Report.* HMSO, London
Department of Health (2002) *Implementing the Caldicott Standard Into Social Care.* HSC 2002/003: LAC (2002)2. The Stationery Office, London
General Medical Council (1998) *Good Medical Practice.* General Medical Council, London
General Medical Council (2000) *Confidentiality: Protecting and Providing Information.* General Medical Council, London
NHS Executive (1996) *The Protection and Use of Patient Information.* HSG (96) 18. NHS Executive, Leeds
NHS Executive (1999) *For the Record.* HSC 1999/053. NHS Executive, Leeds
Thorp J, Walker P (2001) Building confidence: an updated plan for delivering a secure and confidential NHS. *Br J Healthcare Computing Information Management* **18**(5): 17–19