Protecting and using patient information: the role of the Caldicott Guardian

Anne Greenough and Helen Graham

Anne Greenough
MD(Cantab) DCH FRCP FRCPCH, Professor of Neonatology and Clinical Respiratory Physiology

Helen Graham
DCH FRCGP, Head of Quality

Guy's, King's and St Thomas' School of Medicine, King's College London

Clin Med 2004;**4**:246–9

ABSTRACT – All patient information is confidential and must be protected and used appropriately by all members of the healthcare team. Caldicott Guardians have a strategic, advisory and facilitative role to ensure that the Caldicott Principles underpin the approach organizations develop to protect and use patient identifiable information. It is essential all staff and students receive appropriate training and are aware that the responsibility for protecting and using patient information lies with the organisation headed by the Chief Executive and with each individual.

KEY WORDS: Caldicott principles, patient identifiable information

Confidentiality is central to the trust between patients and doctors. All patient information is confidential and must be protected and used appropriately by all members of the healthcare team. This applies not only to clinicians, but also to undergraduate and postgraduate students working in clinical areas and to those undertaking research. Trusts are responsible for ensuring that all their staff are aware of the issues around data protection and confidentiality. The onus rests with medical schools to ensure confidentiality issues are taught and that students have understood their implications

Key Points

Patient identifiable information is any information which allows identification and access to a patient

Patient identifiable information should only be used when absolutely necessary and the minimum required should be used

Access to patient identifiable information should be on a strict need-to-know basis and everyone must understand their responsibilities

Password protection of a computer is not sufficiently secure to protect non-anonymised data

Caldicott Guardians have a strategic role in developing a security and confidentiality policy, as well as responsibility for agreeing and reviewing protocols governing the protection, use and transfer of patient identifiable information

The Caldicott Report

The Caldicott Committee's report contains six principles which underpin the approach that NHS organisations should develop regarding protecting and using patient identifiable information:[1]

- Justify the purpose(s) for using patient identifiable information.
- Only use it when absolutely necessary.
- Use the minimum that is required.
- Access should be on a strict need-to-know basis.
- Everyone must understand their responsibilities.
- Understand and comply with the law.

This means that proposed uses or transfers of patient identifiable information should be scrutinised and continuing uses regularly reviewed. Patient identifiable information should not be used unless there is no alternative, and each item of information should be justified, with the aim of reducing identifiability. Access to patient indentifiable information should be restricted to those staff who have a justifiable need to know in order to effectively carry out their jobs[1] and their access should be limited to only that which they need to see. Action should be taken to ensure that both clinical and non-clinical (for example NHS secretaries) staff are aware of their responsibilities to protect patient confidentiality. Someone in each organisation, usually the Caldicott Guardian (see below), should be responsible for ensuring that the organisation complies with the legal requirements.

Caldicott Guardian

The Caldicott Committee's report on the Review of Patient Identifiable Information highlighted the patchiness of compliance with the full range of confidentiality and security requirements across the NHS. They recommended that raising awareness of these important issues could be facilitated, and to a degree managed, through the development of a network of organisational guardians (Caldicott Guardians). The Caldicott Committee recommended that other organisations which shared NHS patient information should nominate a senior officer to be a Caldicott Guardian. The person specification for Guardians

within NHS institutions was outlined in HSC 1999/012.[2] They should be, in order of priority:

- an existing member of the management board of the organisation
- a senior health professional
- an individual with responsibility for promoting clinical governance.

The Caldicott Guardians were to have a strategic role in developing a security and confidentiality policy, as well as responsibility for agreeing and reviewing internal protocols governing the protection and use of patient-identifiable information and disclosure of patient information across organisational boundaries. Essential to the understanding of the Guardian role is an acceptance that the responsibility for protecting and using patient information lies with the organisation headed by the chief executive and with each individual member of staff.

Upon appointment, the Guardian, working with the information security officer and other support staff, carry out an audit of existing systems and procedures relating to confidentiality and security in the organisation.[1] This is then used as a baseline and an improvement plan is developed. At the end of each year an out-turn report (management audit) is produced to assess current performance and progress against the improvement plan. The management audit provides an assessment of the organisation's performance and capacity by rating the current performance from 0 to 2 against 18 headings, which include safe haven procedures, security monitoring and incidents, reviewing information flows, staff induction procedures and training provision. The Caldicott Guardian of each NHS institution, through their executive board, annually submits the results of the management audit centrally.

Patient identifiable information

Patient identifiable information (PII) is any information which allows access to a patient. Such information includes the patient's name, address, postcode, date of birth, NHS or medical records number, and should be removed when data are used for teaching or research. PII must not be stored on a personal computer; patient information held on a computer must be anonymised. If it is necessary to identify a particular subject, then a unique study number should be given. Password protection of a computer is not sufficiently secure to protect non-anonymised data.

Sharing patient identifiable information

Sharing patient information within and between partner institutions can be vital to the provision of coordinated care to an individual. It is essential, therefore, that institutions have a framework for the secure and confidential sharing of information between agencies, which meets the needs of service users and is in accordance with national and local policies and legislative requirements. Key legislation includes the Data Protection Act 1998, Access to Health Records Act 1990, Crime and Disorder Act 1998 and the Common Law Duty of Confidentiality. The duty of confidentiality requires that unless there is a statutory requirement or other legal reason to disclose information that has been provided in confidence, information should only be disclosed for the purposes that the subject is aware of and for which s/he has given consent.

Consent to share patient identifiable information

Express consent is usually needed for information sharing but not when it is required for activities directly contributing to the diagnosis, care and treatment of an individual. If it is for the benefit of the patient, information can be shared within the multidisciplinary team caring for the patient, but this does not extend to research or teaching or to unqualified members of the clinical team. NHS Trusts, therefore, need to have policies regarding undergraduate students and access to medical records. Patient information can be shared without express consent when justified in the public interest; the courts decide on a case-by-case basis what is in the public interest. It is possible to share information without express consent if the purpose is to prevent serious harm to the physical or mental health of any person or to prevent or enable detection of a serious crime. Express consent is required if information which identifies the patient is used for research, teaching, financial or other management activities. This, for example applies to putting patient identifiable information on a computer (even with encryption) in a database which will be used for examinations or audits.

When seeking consent, it is important to understand who is able to take a decision on behalf of another person. The general rule is that no other person can consent on behalf of an incapacitated adult. The test for capacity includes that the person:

- understands the reasons why there has been a request to share information
- can retain the information
- can weigh up the information and come to a decision.

Children can give consent if they are less than 16 years of age but assessed to be Gillick competent, that is of sufficient maturity, intelligence and understanding to weigh up the factors and fully appreciate their decision. Consent can be given on their behalf, if they are deemed not to be Gillick competent, by an appointee of the court or a person with parental responsibility, that is the mother or the father if he is married to the mother even if they have later been divorced or if not married to the mother has been given formal responsibility via the mother or the court.

Transfer of patient identifiable information

It is essential that adequate precautions must be taken to ensure confidentiality, for example the NHSNet protocol and encrypting Internet email. Sensitive mail,[4] which would have been delivered by hand, should not be sent by email. All faxed information should be subject to Safe Haven procedures, which have been set up in the NHS to ensure that confidential patient data can be

transmitted and stored securely. The Caldicott Guardian must make certain that protocols are in place to ensure that transfer of patient identifiable information is only done appropriately. Locally, this has involved the development of a proforma on which all requests are made to the Guardian and his/her committee. On the proforma, applicants must detail of the nature of information they wish to transfer, with justification for each item. Completing this formal process has helped to minimise the amount of patient identifiable information transferred, by pointing out that at least some of the information was unnecessary for the purpose requested.

Teaching clinicians about confidentiality

Confidentiality issues can be presented in the clinical context through discussion between junior staff and supervising medical staff. This might make formal teaching unnecessary, but that assumes that clinical teachers fully understand confidentiality. The NHS Trust Caldicott Guardians, in completing their annual management audits, report whether systematic assessment of staff training needs occurs, if in-house training is provided, and whether the training has been evaluated.

When this exercise was initially undertaken locally, it revealed that while all new staff received information about Caldicott and Data Protection issues, existing staff did not. A survey of consultant staff revealed that, although 96% were aware of the Data Protection Act 1998 with an adequate/operational level of knowledge, only 58% were aware of the Caldicott report, and they rated their mean level of knowledge of the report as little or none. Yet 88% of the consultants held some form of patient identifiable information electronically, and these consultants were more likely to indicate that they had training needs ($p = 0.031$, Chi square test). Fifty six per cent held patient identifiable information on computer for research purposes and were significantly more likely to store data off-site ($p = 0.0006$), the obvious culprits being portable computers! As a consequence of the results of the survey, training days given by the Caldicott Guardian, Data Protection Officer, Patient Information Lead, were initiated for all levels of staff.

Teaching students about confidentiality

Medical schools must ensure confidentiality issues are taught and, by assessment, determine whether their students have understood their implications. This process can be facilitated by appointment of a medical school Caldicott Guardian, who can also link with the NHS Guardians of partner trusts. Recent graduates should be adequately prepared in confidentiality issues during their undergraduate course, but this cannot be assumed and it is important to ensure that confidentiality issues are covered in the induction courses for pre-registration house officers. All registered doctors receive a set of the GMC guidelines booklets; the two particularly referring to confidentiality issues are *Good medical practice*[3] and *Confidentiality and protecting and providing information*.[4] Senior postgraduate students, however, frequently come from a variety of backgrounds and may not have had sufficient exposure to teaching on confidentiality issues. Postgraduate students at Guy's, King's and St Thomas' were therefore informed of the issues by incorporating a confidentiality statement into the postgraduate handbook. The statement was a simple declaration of confidentiality issues in relation to clinical practice, teaching and research, and included patient clerking, course projects, assessments and general behaviour within and outside the medical school and NHS environment. A sample protocol from the Caldicott Report was used in developing the statement. The confidentiality statement had been drafted with reference to current teaching materials,[5,6] guidance from accredited professional bodies[3,4,7] and a literature search. To determine whether the information given on confidentiality had been assimilated, questions were incorporated into the documentation completed with each student by a higher degrees coordinator at their annual assessment.

Confidentiality and disciplinary issues

For NHS employees, breaches of confidentiality constitute professional misconduct, which is subject to the disciplinary code of the employing Trust. Guidance from the General Medical Council (*The management of doctors with problems: referral of doctors to the GMC's fitness to practice procedures*[5]) states that most performance, conduct or health problems are best handled locally. If the alleged offence may constitute gross (personal) misconduct, including improper disclosure of confidential information, then the guidance indicates that particular consideration should be given to reporting it to the GMC. Initial breaches by students may be managed as a formative educational experience by the dean of medical school, but the student should be warned of the consequences of further breaches – the maximum penalty being exclusion. The severity of the maximum penalties emphasises the importance given to respecting patient confidentiality.[10]

Acknowledgements

We are grateful to members of the Caldicott committees of King's College Hospital and Guy's, King's and St Thomas' School of Medicine, particularly Ms Leigh Howard and Ms Celia Whitchurch and for useful discussion with other Guardians and Data Protection Officers when producing Sharing of Information policies. We thank Ms Deirdre Gibbons for secretarial assistance.

References

1 Caldicott Committee. *Reprot on the review of patient identifiable information*. www.doh.gov.uk/ipu.confiden/index.htm
2 NHS Executive. *Protecting and using patient information. A manual for Caldicott Guardians.* London: NHS Executive.
3 Department of Health. Caldicott Guardians. HSC 1999/012. London: DH, 1999.
4 NHSNet protocol. website: www.nhsia.nhs.uk/def/home.asp
5 General Medical Council. *Good medical practice*. London: GMC, 2001.
6 General Medical Council. *Confidentiality*. London: GMC, 1995.
7 Boyd KM, Higgs R, Pinching AJ (eds). *The new dictionary of medical ethics.* London: BMJ Publishing Group, 1997.

8 Gillon R. Confidentiality. In: Singer P (ed), *A comparison of bioethics*. Oxford: Blackwell, 1998:425–31.
9 Royal College of Psychiatrists. *Good psychiatric practice: confidentiality*. London: Royal College of Psychiatrists, 2000.
10 General Medical Council. *Confidentiality: proctecting and providing information*. London: GMC, 2004.