Confidentiality and medical records

R. V. H. JONES, MA, MRCGP
General Practitioner, Seaton, Devon; Senior Lecturer, Department of General Practice, Postgraduate Medical Institute, University of Exeter

S. JANE RICHARDS, MRCGP, DCH, DRCOG
General Practitioner, Exeter

SUMMARY. Protecting confidential information disclosed to doctors has been one of the most important ethical traditions of the medical profession. However, the patient's right to such confidentiality is threatened because it is legally unclear how far ownership by Government of the paper on which NHS records are kept or of the computer system in which they are stored confers right of access.

We hope the medical profession will examine this problem urgently and offer some suggestions as to how patients' confidences can continue to be protected in the future.

Introduction

BOTH patients and doctors assume that, unless specifically stated otherwise, the information exchanged during a consultation is confidential and will not be divulged without the patient's consent. This assumption includes the records made as a result of the consultation. There are four recognized exceptions.

First, the doctor has a statutory duty to report prescribed industrial and infectious diseases as laid down in the Factories Act (1961) and the Factories (Notification of Diseases) Regulations (1966). Secondly, he must reveal confidential information if ordered to do so by a court. Thirdly, discussion with a close relative or friend may be undertaken by the doctor if this is thought to be in the patient's best interest. Fourthly, although not yet tested in the courts, it is recognized in practice that a doctor may disclose information about a patient if he believes there is potential danger to the community which outweighs the principle of confidentiality.

Maintaining the patient's confidence

When a general practitioner refers a patient for a specialist opinion the patient's consent is implicit as the patient is aware of what is happening and realizes that it is necessary that the consultant should have information in order to form an opinion. Apart from these exceptions, information should not be disclosed to third parties without the patient's consent.

There are ethical, legal and practical reasons why this position should continue.

1. *Ethical*

The ethical position was first stated by Hippocrates 2,500 years ago: "Whatever in connection with my professional practice or not in connection with it I see or hear in the life of men which ought not to be spoken abroad I will not divulge, as reckoning that all such should be kept secret." The Hippocratic oath was restated in modern language in the Declaration of Geneva in 1947. The ethical position has subsequently been reaffirmed by resolutions of the Representative Body of the British Medical Association (BMA, 1977) and is quoted in the pamphlet *Professional Conduct and Discipline* published by the General Medical Council (1977).

2. *Legal*

Since the case of Kitson versus Playfair in 1896, when a medical practitioner was found guilty of "breach of an implied covenant of secrecy" and had to pay damages of £12,000 (Martin, 1973), the doctor-patient relationship has had a legal as well as an ethical liability. This was reaffirmed in a case brought to the disciplinary committee of the General Medical Council in 1971 when a general practitioner was accused of improperly disclosing information to the parents of a 16-year-old girl about her treatment. The judgement was based on "the particular circumstances of the case" but upheld

"the general view that information about a patient should not be disclosed without the patient's consent" (*British Medical Journal,* 1971).

3. Practical

Unless in practice a patient could be sure that anything he told a doctor would be treated as confidential, he might fail to divulge something relevant to his illness (*Journal of the Royal College of General Practitioners,* 1973). Furthermore, unless the doctor felt that the information contained in the records was safe from scrutiny by a third party, he might either fail to record or might record all 'sensitive data' on separate private files.

Present position

In general practice the fact that patients' records are kept on the premises and that there are relatively few professional staff involved in looking after each patient has made maintenance of confidentiality comparatively easy. There may be room for misgiving about the readiness with which some general practitioners send away patients' notes at the request of insurance companies, and also at the arrangements for maintaining confidentiality in the future as the numbers of professionals in practice and practice teams increase, but most general practitioners are well aware of their responsibilities.

In occupational and industrial medicine both medical officers and employers have in general accepted that while an employer is entitled to a medical opinion about an employee (with the employee's consent), the information contained on the medical record is the property of the medical officer.

A legal opinion by Mr (later Justice) James Sterling QC in 1961 supported the view that, although the employer may have legal ownership of the medical records of his employees, this does not give him the right of unrestricted access, since such access would infringe the rights of the employee (*Transactions of the Association of Industrial Medical Officers,* 1962).

In hospital practice there are difficulties. There are many more staff involved in the care of an individual patient, often from several different departments; medical records are thus more easily available to a greater number of people than in industrial medicine or in general practice. As a result of this it is likely that awareness of the importance of confidentiality may become blunted.

Ethically, however, the position is clear. The clinician in charge of the patient is responsible for the confidentiality of the medical record, as it is to him or for him that the information is given for the purpose of the clinical care of the patient. The legal ownership of the record, however, rests with the Secretary of State of the Department of Health and Social Security, and through him with the hospital administrator or his successor the district administrator.

Problems

1. Right of access and ownership

The paper on which the records of private patients are kept belongs to the doctor. However, the paper on which NHS records, both in general and hospital practice, have been written belongs to the DHSS. Thus, the question arises—what rights does 'ownership' confer? Does ownership of the paper confer right of access, or the right to grant access to a third party? Certainly general practitioners have never considered that because they write their records on paper which belongs to the Secretary of State that the Secretary of State has the right to inspect the record, or to rule to whom information contained on it might be divulged. This would be contrary both to ethical principles and practice.

With computerization of records becoming more widespread it is likely that medical records will increasingly be held on computers owned by the regional or area health authority at some distance from the consulting room. Such records already exist for immunization and vaccination purposes and there are plans for a standard child health computer-based record. Does ownership of the computer confer the right to know what is recorded on it? In our opinion it is important that the legal position concerning the rights of ownership should be clearly defined in order to prevent legal and ethical problems in the future.

2. Right of access for other purposes

The information contained on medical records is useful not only for the clinical care of the patient but also for research, for planning, and for monitoring services. Information, for example, about the number of handicapped children and the nature of their handicap is necessary for the planning of services within a district or area. Information about single-parent families in relation to perinatal mortality is a legitimate research interest.

The problem is that confidentiality may be breached when information which a patient has given for one purpose is used for another purpose without that patient's consent. The quality of information involved (for example, factual or judicial, sensitive or non-sensitive), and whether the patient is identifiable or not are variables which complicate the situation.

It is important that the profession should agree principles which govern the use to which identifiable and non-identifiable information is put.

3. Transfer of information

When medical information is recorded on paper in a manual system it is both difficult and time-consuming to transfer it to another system, except by photocopying. With information recorded on computers, however, transfer is quick and easy. Medical information collected in one practice or hospital could be transferred to another system at the touch of a button.

Insurance companies, credit-card companies, the vehicle licensing centre at Swansea, the police, and the banks have computer-held records which contain information about identifiable individuals. Much of this is sensitive and personal. How well is this information protected at present? Is access by third parties possible? Can data be transferred from one system to another without the knowledge of either the person involved or the person who placed the information on record?

In our view, the establishment of rules governing the transfer of information and, in particular, information derived from medical records, is now vital.

Possible answers

It has been recognized for some time that when computers came into general use for storing information, problems about confidentiality and the invasion of privacy would arise.

The Younger Committee on Privacy (1972) published ten principles which they considered necessary to safeguard the privacy and accuracy of information (including medical information) held on computers. In December 1975 the Government published the White Paper *Computers and Privacy* which took note of the Younger principles, recognized the special position of medical records, and recommended that a Data Protection Committee be established which would consider evidence and recommend measures to be incorporated in an Act of Parliament. The purpose of the proposed Act would be to establish permanent statutory arrangements to protect information held in computer systems. The Data Protection Committee was appointed in 1976 and is still deliberating.

Policy of the BMA

The British Medical Association submitted written evidence in October 1976 and oral evidence in April 1977. It argued that where medical records are stored on computers the safeguards for maintaining confidentiality should not only be maintained but strengthened.

The Younger Committee in 1972 had among other things suggested that records should be held for a "specific purpose" and should not be used for any other purpose without "appropriate authorization."

Following these principles the BMA submitted the following clarifications:

1. Information on medical records should be regarded as held for the "specific purpose" of the *continuing care of the patient.*

2. Information on medical records should not be used for any other purpose without "appropriate authorization" by *the person clinically responsible for the care of the patient (or his successor with clinical responsibility) or the consent of the patient.*

3. Access to information should be confined *to those authorized to have it for the purpose for which it was supplied.*

If these principles are accepted it would follow that when records or parts of records are used for purposes other than the purpose for which the information was supplied then the records must not be identifiable. For instance, identifiable clinical records should not be used to provide information for planning purposes. Neither should they be used for research unless a follow-up of the individual patient is a necessary part of the research.

The first and third principles are derived directly from the ethical considerations which apply to all consultations. With regard to the second principle, it could be argued that information from which all means of identification had been removed could be used quite properly for purposes other than those for which it had been supplied without either "appropriate authorization" or the patient's consent. For example, information about old people living alone who were unable to climb stairs could be useful both to the social services and to the housing departments. However, we believe, in line with the evidence of the BMA, that if information is given by a patient to a doctor in the course of a consultation then that information, even if rendered unidentifiable, should not be used for purposes other than the care of the patient without the consent of the clinician or the patient. If the information is made unidentifiable the responsibility for maintaining confidentiality should rest with the clinician.

Applications

In the Oral Contraception Study, carried out by the Royal College of General Practitioners, the patient's permission was sought to use unidentifiable clinical information for research. Each general practitioner involved in the study sent anonymous information to the Manchester Research Unit of the Royal College of General Practitioners. The key and code which identified each patient was known only to the general practitioner concerned (RCGP, 1974). In this large research project the precautions taken to ensure confidentiality were in retrospect totally consistent with the principles now proposed by the BMA.

In hospital practice there is a distinction between clinical medical records which contain personal often sensitive information about individual patients and those hospital records which are necessary for monitoring the services provided by the hospital, such as length of time on waiting lists, length of inpatient stay, or the amount and type of day-case surgery. In our view, the adoption of the second principle would confirm the responsibility of the clinician for maintaining confidentiality of clinical records while permitting records of hospital activity to be used for monitoring and planning methods of maintaining confidentiality.

Primary and secondary records

Crombie (1973) was the first to suggest a system of primary and secondary records as one way to approach the general problem of confidentiality in research. He

proposed the division of records into primary records, which are individual, identifiable, and used in the clinical care of the patient, and secondary research records which are coded and are not identifiable except by the clinician who knows the key.

Although this system was suggested for use in research it could also be extended so that, while the patient's code would continue to be known to the doctor, the information needed for planning or monitoring could be put on a series of secondary files. When clinical records are held on a computer, there is an alternative solution. Instead of coding the patient it is possible to code the person seeking information. Any part of a computer record, including means of identification, can be made accessible or inaccessible depending on the code used by the person seeking information. This type of system is currently in use in two group practices in Devon where all the patients' records have been placed on a computer (Bradshaw-Smith, 1976).

Recommendations

Other ways of solving the technical difficulties of maintaining confidentiality of records will undoubtedly be devised. At present the danger is that unless principles such as those suggested by the BMA are discussed and accepted by the profession as a whole, the confidentiality which both patient and doctor at present *assume,* and which forms the basis of the doctor-patient relationship, will under various pressures be quickly eroded.

Community physicians have their responsibility to the community for its collective health. National Health Service specialists are salaried and ultimately responsible to the NHS for the care of those patients who come to the hospital in which they work.

As general practitioners and independent contractors, we have a direct and continuing relationship with our individual patients. We are, therefore, in the front line when it comes to issues of confidentiality and the individual. We believe that general practitioners should not only continue to accept responsibility for their patients' records, with all the consequences that this implies, but should also take the lead in proposing working principles which could be accepted by the profession as a whole. We therefore recommend that:

1. The Royal College of General Practitioners should press for acceptance of the principle that ownership of the paper or machine on which medical information about individuals is stored does not confer right of access to the record.

2. The Royal College of General Practitioners should examine and, if agreed, publicly endorse the three principles submitted to the Data Protection Committee by the British Medical Association.

These recommendations are in agreement with those made in 1973 by the Awards and Ethical Committee of the Royal College of General Practitioners (Donovan *et al.,* 1973).

References

Bradshaw-Smith, J. (1976). *British Medical Journal,* **1,** 1395-1397.

British Medical Association (1974). *Medical Ethics* pp. 13-14. London: BMA.

British Medical Journal (1971). Supplement No. 1, pp. 79-80.

Computers and Privacy (1975). Cmnd. 6353. London: HMSO

Crombie, D. L. (1973). *Journal of the Royal College of General Practitioners,* **23,** 863-879.

Donovan, C., Grant, D., Woodhall, J. & Zander, L. (1973). *Journal of the Royal College of General Practitioners,* **23,** 881-885.

General Medical Council (1977). *Professional Conduct and Discipline,* p. 16. London: GMC.

Journal of the Royal College of General Practitioners (1973). Editorial, **23,** 833-839.

Martin, C. R. A. (1973). *The Law relating to Medical Practice.* London: Pitman Medical.

Royal College of General Practitioners (1974). *Oral Contraceptives and Health.* London: Pitman Medical.

Transactions of the Association of Industrial Medical Officers (1962). **11,** 186.

Younger, Sir K. (1972). *Committee on Privacy.* Cmnd. 5012. London: HMSO.

Addendum

Dr R. V. H. Jones is a member of the General Medical Services Committee and Dr Jane Richards is a member of the Council of the British Medical Association. They were two of the representatives of the British Medical Association who gave oral evidence to the Data Protection Committee. The opinions they express in this article are their own except where they quote from the policy of the BMA.

The Data Protection Committee is expected to publish its report soon. Whatever its recommendations, we believe that the medical profession should discuss widely the implications of the effects of changing circumstances on medical confidentiality.

Dextroamphetamine with morphine for the treatment of postoperative pain

In a double-blind, single-dose study, dextroamphetamine combined with morphine was compared with morphine alone to determine the relative efficacy of the combination given intramuscularly for postoperative pain. Each of 450 patients received one treatment of morphine sulphate (3, 6 or 12 mg) with dextroamphetamine (0, 5 or 10 mg). Analgesia, as measured by the patients' subjective responses to questions about relief of pain, was augmented when dextroamphetamine was given with morphine; the combination of dextroamphetamine, 10 mg, with morphine was twice as potent as morphine alone, and the combination with 5 mg was one and a half times as potent as morphine. In simple performance tests, and in measures of adverse effects, dextroamphetamine generally offset undesirable effects of morphine (sedation and loss of alertness) while increasing analgesia. Effects on blood pressure, pulse and respiratory rate were minimal.

Reference

Forrest, W. H., Brown, B. W., Brown, C. R. & Defalque, R. (1977). *New England Journal of Medicine,* **296,** 712-715.