Application of the privacy principles to general practice

Ea Mulligan, Wendy Rogers, Annette Braunack-Mayer

Ea Mulligan, MBBS, BMedSci(Hons), MHAdmin, AFACHSE, FRACGP, FRACMA, is a PhD candidate, School of Law, Flinders University of South Australia.
Wendy Rogers, MBBS, BAHons, PhD, DipRACOG, MRCGP, FRACGP is Research Fellow, Department of General Practice, Flinders University of South Australia.
Annette Braunack-Mayer, BMedSci(Hons), PhD, is Lecturer, Department of Public Health, University of Adelaide.

BACKGROUND There are escalating requirements for general practitioners to comply with recognised privacy principles. With amendments to the Commonwealth Privacy Act (1988) imminent, there is an urgent need to formulate methods for applying these principles to general practice.
OBJECTIVE The article provides an explanation of the origins of the privacy principles and a simple self audit which general practitioners can use to assess the extent to which their usual practices conform with them.
DISCUSSION A careful review of the principles indicates that new measures will be needed before most general practices will be able to approach required standards of conduct. Practical strategies for achieving best practice are discussed and challenges confronting general practices in applying the principles are canvassed. Ethics committees should be used more often to provide independent review of practice policies and proposals to use patient information in new ways. General practitioners can expect increasing scrutiny and debate concerning confidentiality. In order to maintain patient trust in GPs as responsible data custodians, the privacy principles can be seen as a quality improvement tool.

Received 29 June 2000; accepted 15 August 2000

Confidentiality and patient consent are important ethical issues in the management of patient information in general practice. Previously we have discussed these issues with regard to research and evaluation.[1,2] This article examines these issues in relation to the privacy principles and routine general practice care.

This work has new urgency because amendments to the Commonwealth Privacy Act (1988), extending its application to all private sector organisations (including general practice) are before parliament at the time of writing. Information management practices which have been accepted previously do not conform to the requirements of the Information Privacy Principles found in Section 14 of the Act.

Although confidentiality is highly valued by both patients and general practitioners, there is little evidence as to the effectiveness of current measures used to protect it. There are generalised public concerns that privacy is being eroded and that the expanding use of electronic information technology has made information more vulnerable to misuse.[3]

While a majority of Australians express confidence in health care providers, an important minority are not confident that doctors and hospitals are responsible data custodians. In individual cases this is often associated with embarrassment or other harm to the patient, although most adverse events do not result in any formal complaint or legal action.[4]

Origins of the privacy principles

International privacy principles were initially proposed as a mechanism to facilitate the international transfer of personal information. They were intended to support community confidence and to harmonise privacy regulations. The Organisation for Economic Cooperation and Development (OECD) issued a series of guidelines intended to assist its members to develop consistent legislation in relation to the handling of personal data. The first of these[5] formed the basis for the Information Privacy Principles found in Section 14 of the Commonwealth Privacy Act 1988 which applied mainly to Commonwealth agencies. A subsequent

Table 1. Compliance self audit

- We will only collect information that is necessary for what we do
- We will be fair in the way we collect information about you
- We will tell you who we are and what we intend to do with the information about you
- Where practicable, we will collect personal information directly from you
- If we collect information about you from someone else we will, whenever possible, make sure you know that we have done this
- We will only use or disclose information about you in ways that are consistent with your expectations or are required in the public interest
- We will ensure that information about you is accurate when we collect or use it
- We will keep information about you secure
- We will be open with you about what kinds of personal information we hold and what we do with it
- Wherever possible we will let you see the information we hold about you and correct it if it is wrong
- We will limit the use of identifiers that government agencies have assigned to you (eg. Medicare number)
- If we can (and you want to) we will deal with you anonymously
- We will take steps to protect your privacy if we send personal information about you to a third party
- We will limit the collection of highly sensitive information about you

Headings from *National Principles for the Fair Handling of Personal Information* 1999 produced by the Australian Privacy Commissioner and available from the Human Rights and Equal Opportunity Commission.

European Union Directive[6] has called for regulation of both public and private sectors.

The privacy principles have been adopted in modified form by some state governments and are incorporated to varying extents into a number of recognised health standards.[7-10]

The Australian privacy principles articulated in the Privacy Act (1988) are generic. Intended to apply to a broad range of industries, they require some interpretation in order to understand their application to general practice. Medical records must be understood as 'personal information', GPs and practice staff become 'data gatherers' and GPs are also 'data custodians'. Despite this unfamiliar terminology, the underlying concepts of confidentiality and respect for patient autonomy can easily be recognised.

Application of the privacy principles

A plain English version of the privacy principles has been produced by the Australian Privacy Commissioner.[11] They can be used in a simple self audit of compliance with the principles. Ask yourself whether these undertakings could honestly be made to a patient of your practice (*Table 1*). For GPs some of these statements are not problematic, while others would be very challenging to use.

For general practices seeking to apply the privacy principles, one useful strategy would be to formulate a practice policy on confidentiality. Such a policy should address:

- staff responsibilities
- informing patients
- recording consent
- patient access to records, and
- a procedure for obtaining ethical review for any activities which may breach one of the privacy principles.

Staff responsibilities

General practitioners and their practice staff will require education about the responsibilities of information collectors. They must ensure that information is relevant, up to date and complete and that the record is protected securely. They are also responsible for assisting patients to find out what records are kept about them and who may have accessed these records.

Informing patients

General practitioners and reception staff collecting personal information from patients should make them aware of the purposes for which the information will be used and who will have access to it. The RACGP has recently released a patient education pamphlet titled *Personal Information Privacy and your General Practitioner** which could be provided to patients by the reception staff at the time that information collecting begins.

Patients need to be informed that they are entitled to have access to records about them and that they may request corrections or additions to inaccurate or misleading information. If done well, this will establish implied or explicit consent by patients to routine information management practices.

Obtaining consent carries with it the certainty that some patients will not consent. Methods for providing care to these patients will need to be provided. For some, concerns can be overcome by offering to keep minimal or limited records of the most essential information. Others will be reassured when they can read all of the records of a consultation before leaving and understand that nothing harmful or disparaging has been recorded. Providing a patient with a pseu-

*Copies of this pamphlet are obtainable by contacting Ms Robyn Cronolly on (03) 9214 1414.

donym or coded identifier (eg. mother's maiden name or last two letters of first name/birth month/last two letters of family name) are simple methods for providing nonidentifying care.

Recording consent for information transfers

Coordination and integration of care requires sharing patient information with other service providers. Consent by the patient is required for this process. Acting on this consent will require record keeping systems which will flag information patients have consented to release, and will identify data patients have indicated require special privacy measures.

In practical terms, it may not be possible to comply with a patient's request to restrict distribution of information about them. General practitioners have limited control over the security of patient information which they provide to other organisations, such as diagnostic services and hospitals. The more that data transfers between systems are automated, the less ability there is to stop data on a particular individual being transferred from one data repository to another.

Patient access to records

Patient access to medical records is not universally accepted by GPs. However, this will become mandatory if the provisions of the Privacy Act are extended to the private sector. All state health services have processes which allow patients to routinely access their health records. General practitioners operating in the public sector have not reported any particular difficulties arising from this.

Ethical review of new uses for patient information

It is often difficult to tell patients what their information will be used for. Not only may new uses be developed for information after it is collected, but data collection starts at the reception desk where details such as name and address may be directed into a number of different information systems (billing, ordering diagnostic tests, electronic prescribing).

General practitioners have to consider the implications of proposals to link patient data in new ways, the use of data for new purposes and the accessing of data by new people. The results of these decisions will be the subject of increasing scrutiny and debate.

Any new use of patient data requires consent from the patient. In addition, any use of information which may breach one of the privacy principles must become the subject of independent review. Ethics committees represent a significant source of expertise and they are able to provide independent determinations. Consideration of information policies and adjudicating on proposals which seek to use patient data in breach of any of the privacy principles are tasks which need to be referred. This poses a problem for GPs who do not have access to an institutional ethics committee.

Conclusion

The expectation that the treatment of health information in general practice will conform to the privacy principles will increase as the principles are incorporated more extensively into legislation, codes and standards. A careful review of the privacy principles indicates that new measures will be required before most general practices will be able to approach required standards of conduct.

An overall change in climate reflecting a decreasing level of paternalism and increasing patient autonomy will result in demands from patients and their advocates for more explanation of the uses to which information will be put. There will be growing expectations that patients will be able to review information, verify security, scrutinise audit trails and be treated anonymously.

If it is kept clearly in mind that the ultimate goal is to maintain the high level of trust which Australians have in GPs, the privacy principles can be seen as a quality improvement tool. Their application will strengthen many other developments in health which acknowledge patient autonomy and seek to engage patients as active partners in the project of improving health.

References

1. Braunack-Mayer A, Rogers W A. Handling information ethically: some strategies for discussion. Aust Fam Physician 2000; 29(10): 1005–1008.
2. Rogers W A, Braunack–Mayer A. Handling information: some ethical issues. Aust Fam Physician 2000; 29(8): 806–808.
3. Privacy Commissioner. Community attitudes to privacy. Canberra: Human Rights and Equal Opportunity Commission, 1995. Report No: Information Paper Number 3.
4. Mulligan E. Confidentiality in health records; evidence of current performance in the South Australian health system. Poster presentation, Australian College of Health Service Executives Annual Convention 2000; 8th–9th June, Stadium Australia, Homebush, 2000.
5. Organisation for Economic Cooperation and Development. Guidelines on the protection of privacy and transborder flows of personal information. Paris: 1980.
6. European Parliament, Council of the European Union. The protection of individuals with regard to the processing of personal data and on the free movement of such data. 95/46/EC.
7. Standards Australia. AS 4400–1995: Personal privacy protection in health care information systems. Homebush: Standards Australia, 1995.
8. Royal Australian College of General Practitioners. Code of practice for the management of health information in general practice. Melbourne: RACGP, 1998.
9. NSW Health Privacy of Information Committee. Information privacy; code of practice. Sydney: 1996.
10. Royal Australian College of General Practitioners. The RACGP standards for general practices. 2 edn: RACGP, 2000.
11. Office of the Privacy Commissioner. National principles for the fair handling of personal information. Sydney: Human Rights and Equal Opportunity Commission, 1999.