Complying with the Privacy Act

A survey of medical records management

Ea Mulligan, *BMBS, BMedSci (Hon), MHealthAdmin, FRACGP, FRACMA, AFACHSE, is a PhD Candidate, School of Law, Flinders University, South Australia.*

BACKGROUND A survey of 142 South Australian general practices was conducted on the eve of the new Privacy Act amendments coming into force.

OBJECTIVE The survey had two aims: to establish the extent to which medical records systems were already compliant, and to identify those areas in which change would be required in order to achieve compliance with the requirements of the new legislation.

DISCUSSION The sample was biased in favour of larger group practices. Among the practices surveyed, the areas of best compliance were in providing security, allowing patients access to records and obtaining consent for disclosure of information.There was poor compliance with the requirement to provide patients with information about medical records, or to have a practice policy on privacy. Anonymous care was rarely offered to patients. General practices will need to develop policies and procedures to address these requirements of the new law. Some general practices met the standard required by the amended Privacy Act before it came into force. For those who were not compliant, relatively simple measures will overcome the most common deficiencies.

The provisions of the Commonwealth Privacy Act 1988 were amended to apply to all private medical practices in Australia from 21st December 2001.

Amendments to the 1988 Commonwealth Privacy Act were considered by committees in both houses of parliament and there were many submissions concerning the effects the new provisions would have on medical practice.[1] Some argued that medical practitioners and other health care providers already provided a very high standard of confidential care, that they generally treated patient information with discretion and were not in need of any further regulation. There was brisk debate about whether patients should have the right to access medical records. Representatives of the medical profession argued that patients' access to medical records should be limited.

A survey of private medical practices in South Australia was conducted on the eve of the new provisions coming into force. It sought to establish the extent to which private medical records systems were already compliant and to identify those areas in which change will be required in order to achieve compliance with the requirements of the new legislation. The results are accompanied by a condensed version of the National Privacy Principles and some suggestions as to simple measures which general practitioners can take to improve compliance.

Methods

Six hundred and ninety-eight questionnaires were mailed to private medical practices during October 2001. Practices were selected randomly from entries in the metropolitan and country Yellow Pages directories. There were 260 questionnaires returned (37%), of which 142 were from general practices.

Questions were designed to audit compliance with the main requirements of the National Privacy Principles embodied in Schedule 3 of the Act (Table 1).

Results

1 and 10: Collection of sensitive information

'At the time that information is gathered for medical records, are patients made aware of the uses which will be made of these records?'

Ninety-eight (69%) of the general practices surveyed indicated that patients were not informed what their medical records would be used for. Seventeen (12%) indicated that patients were routinely informed while a further 27 (19%) indicated that patients would sometimes be informed. Overall, less than one-third (31%) of these general practices reported that any of their patients were made aware of the possible uses of their medical records.

'At the time that medical records are created, are patients advised of any other people or organisations who may later

gain access to the information – for instance practice staff or other treating practitioners?'

Patients were given this advice slightly more often in 49 (35%) of the surveyed practices. Patients may be advised of other people who may later gain access to their information routinely (18: 13%), or sometimes (31: 22%).

Those practices who provided patients with information were asked what measures they took to provide this information. Responses fell into four groups:

- Routine advice: These practices usually provided verbal advice to new patients either via reception staff, or the GP as part of the first consultation.
- Exceptional circumstances: These practices provided information when a later disclosure could be foreseen, eg. workers compensation report or cervical cancer screening registration.
- On request: In these practices, no routine advice was given, but questions would be answered if the patient asked.
- Implicit understanding: Many practices assumed that patients would understand what medical records are used for and who would access them. As one GP wrote: 'We expect them to know'.

2. Use and disclosure

'Excepting mandatory reporting, is consent obtained from patients before information about them is released to persons outside the practice?'

Generally, consent is required for all releases of information to persons outside of the treating team (although there are a few circumstances where the patients consent is not required because information release is compelled or allowed by law).

In most of the general practices (115: 82%) consent for information release was always obtained, while this was done on some occasions in a further 20 (14%) general practices. Only six (4%) of the 141 general practices responding to this question indicated that consent was never obtained for release of information.

A written record was kept of consent to release information in 101 practices (74%) and 20 (14%) practices provided a form for patients to sign to authorise release of their information.

3. Data quality

'Are patient details (such as address and contact telephone numbers) routinely checked and updated: on every presentation by a patient, on the first presentation by a patient, on request by a patient?'

Nonclinical patient information was checked at every presentation by a patient in 83 (58%) of the general practices surveyed.

'Are clinical details (such as current medications) routinely checked and updated: on every presentation by a patient, on first presentation of a new patient, when clinically indicated?'

Clinical information was checked and updated at every presentation by a patient in 64 (45%) of the general practices surveyed.

4. Data security

In almost all (130: 93%) of the general practices surveyed, paper medical records were stored in secure areas at all times; 126 (88%) had electronic patient records, and of these, 119 (98%) required a password for access. Half of the general practices surveyed required their nonclinical staff to sign confidentiality agreements.

5. Openness

Only eight of the 142 general practices surveyed (6%) supplied a privacy policy although a further eight provided a practice information pamphlet that mentioned confidentiality and/or avenues for complaint.

6. Access and correction

Patients were able to read and/or obtain copies of their medical records on request in 86 (60%) of the general practices surveyed, and a further 47 (33%) sometimes provided access. Only 11 (7%) indicated that they never allowed patients access to their medical records.

7. Government issued identifiers

The Privacy Act explicitly prohibits the use of government issued identifiers (Medicare, tax file, pension or veterans' affairs numbers) as a numbering system for medical records. Because these numbers have many digits and are not issued consecutively to the patients of a particular practice, they are not attractive for use. Therefore, the survey did not include any question on their use as a unit record number.

8. Anonymity

'If a patient seeks consultation or treatment without revealing their identity, can this be accommodated?'

Of all the requirements of the new legislation, this appeared to cause some consternation. Eleven (8%) did not answer the question at all, some writing in the margin: 'I have never been asked'. A small group of general practices indicated that they would provide anonymous care on request (8: 6%), while a further 16 (11%) would provide this service under some circumstances. A large majority (107: 75%) indicated that anonymous care was never provided.

9. Transborder data flows

A surprisingly large proportion of general practices (23: 16%) had sent patient information overseas within the previous year. Seventeen out of 23 (70%) gave information to the patient for distribution, while six out of 23 sent information out of Australia to patient's treating practitioners, legal representatives or insurers on receipt of a signed authorisation from the patient.

Discussion

The Yellow Pages directories provided a comprehensive sample set, but contained many duplications. Practices with a number of partners typically had multiple entries, and therefore, multiple opportunities to be recruited. Any conclusions drawn from the survey will be more true of group practices

Table 1. National Privacy Principles[4]

1. Collection and 10. Sensitive information

All health information is considered to be sensitive information and should only be collected with the patient's consent. Practitioners are required to:

- Collect only the information necessary to deliver the health service
- Collect lawfully, fairly and not intrusively
- Obtain a person's consent to collect health information about them
- Ensure that consumers are informed about why their health information is being collected, who is collecting it, how it will be used, to whom it may be given and that they can access it if they wish

2. Use and disclosure

Health service providers may:

- Use health information for patient care and other directly related purposes
- May disclose personal information to others if the consumer gives consent
- Disclosures without consent may be permitted in special circumstances

3. Data quality

- Health service providers are required to take reasonable steps to keep health information up-to-date, accurate and complete

4. Data security

- Health service providers are required to take reasonable steps to protect health information from loss, misuse and unauthorised access

5. Openness

- Health service providers are required to develop a written health information policy and this must be available to anyone who asks for it

6. Access and correction

- Consumers have a general right of access to their own health records
- Consumers may ask for information about them to be corrected, if it is incomplete, inaccurate or out-of-date

7. Identifiers

- Government issued identifiers (eg. Medicare number) may not be used as a unit record number in private records systems

8. Anonymity

- Where lawful and practicable, consumers must be given the option to use health services without identifying themselves

9. Transborder data flows

- Health information may be transferred out of Australia if there is similar privacy protection in the recipient country

Adapted from: Health Information and the Privacy Act 1988. The full text of the Privacy Act 1988 can be found at www.privacy.gov.au

Table 2. Practice tips for Privacy Act compliance

- Educate patients about what medical records are used for and who will have access to the information in them. Give new patients the RACGP pamphlet
- Let patients read or have copies of their records if they ask for them
- Get consent before releasing information to anyone else (unless there is a law which requires or allows you to do so without consent)
- Have a reliable system for updating clinical information (eg. current medication lists)
- Have a written privacy policy available if anyone requests it
- Keep paper and electronic records secure
- Consider how care could be provided anonymously
- Do not use Medicare numbers as medical record numbers

than of the medical records systems of smaller general practices.

On the eve of the application of new privacy legislation, many of the general practices surveyed were already compliant with elements of the new requirements. In a few practices, management of patient information was already at, or above the standard required by the new law.

Of the requirements of the new legislation, security against unauthorised access has received the most attention from general practices. A large majority reported that their medical record systems were secure and almost all of their electronic records systems were protected by passwords. While a password does not guarantee security, it does indicate that an effort has been made provide a secure system.

All but a few general practices sought consent from patients before releasing information about them outside the practice. Many kept a written record of this consent. The prevalence of patients reporting unauthorised release of health information in South Australia is low.[2] From this survey, it appears that confidentiality agreements are not generally in use in general practices. While signing an agreement is a common method for gaining commitment to an employer's policy, they are not required by the Privacy Act.

Maintaining up-to-date information in medical records is time consuming and it has not been established how much effort should go into taking reasonable steps to keep records up-to-date as required by the National Privacy Principle 3. Although checking and correcting records in response to a prompt (as needed, or on request) may produce up-to-date records,

this approach would be expected to produce records with variable levels of currency. The highest standard of maintenance would be to check and correct the existing information on every presentation by a patient. Approximately half of the surveyed practices did this.

There are some difficulties for GPs in strict compliance with the National Privacy Principle 9 (concerning the transfer of information to overseas destinations). There is no easy way for medical practitioners to check on the legal privacy protections in countries to which their patients travel. Indeed, patients may choose to travel to countries where there is no privacy legislation. In the face of these dilemmas, the usual practise of giving a health summary or report to the patient seems prudent. The patient then takes responsibility for controlling distribution of the information and makes their own judgment as to the risks of releasing it at their destination.

Common deficiencies

The survey demonstrated that some of the requirements of the new legislation were not part of generally accepted practice. These are the areas in which change will be needed if general practices are to become compliant with the law as it now stands. Table 2 gives practice tips for Privacy Act compliance.

Information to patients and practice policy

Providing information to patients at the time that records are created and informing them about what medical records will be used for, and who may later gain access to the information in them, is not difficult to achieve. Giving a pamphlet to new patients would easily address this requirement for patient education (see Resources).

Few general practices supplied a written privacy policy. This is a requirement of the legislation. Some practices indicated that they were in the process of developing a policy. The demands of practice accreditation may provide an additional prompt for practices to adopt a written privacy policy. A template for a privacy policy is available from the RACGP website (see Resources).

Anonymous care

One requirement of the legislation which will be novel for many general practices will be offering anonymous care. Some argue this is not practicable because it would preclude raising an invoice or seeking a refund from Medicare or another insurer. This consideration should not restrain practices from offering anonymous care for cash payment. Research conducted in the United States[3] has identified a group of patients who are prepared to pay out-of-pocket for medical services in order to ensure the confidentiality of their health information.

In Australia, many sexual health services provide care to patients using an alias and a small proportion of the general practices surveyed had developed procedures that allowed them to offer anonymous care routinely on request. Practices that have no system for obscuring a patient's identity would do well to seek advice from a service that has them in place.

Complaints process

At the end of the day, the new legislation now provides patients with an avenue for complaint to the Federal Privacy Commissioner. General practitioners should not expect any surprise investigations, since the Privacy Commissioner will not investigate a complaint unless the patient has already contacted the organisation they are complaining about and has not received a satisfactory response after 30 days.

Conclusion

Compliance with the new provisions of the Privacy Act should not be difficult for general practices to achieve. Some practices surveyed had compliant medical records management systems before the legislation came into force. For those that were not compliant, relatively simple measures will overcome the most common deficiencies (Table 2).

Among the practices surveyed, the areas of best compliance were in providing security, allowing patients to access records, and obtaining consent for disclosure of information.

There was poor compliance with the requirement to provide patients with information about medical records, or to have a practice policy on privacy. Anonymous care is rarely offered to patients. General practices will need to develop policies and procedures to address these requirements of the new law.

Ethical clearance and financial support

This research protocol was approved by the Social and Behavioural Research Ethics Committee of the Flinders University of South Australia, and was supported by a research student maintenance grant.

Resources

- AMA Privacy Kit. Available at: http://www.ama.com.au/web.nsf/doc/SHED–5FN6BP
- RACGP Code of Practice and Practice Policy template: Management of Health Information in General Practice. Available at: http://www.racgp.org.au/downloads/doc/20011221leaflet.doc
- Australian Privacy Commission Health Privacy Guidelines. Available at: http://www.privacy.gov.au/

References

1. Commonwealth Senate, Legal and Constitutional Legislation Committee. Report on the provisions of the Privacy Amendment (Private Sector) Bill 2000, and Commonwealth, House of Representatives Standing Committee on Legal and Constitutional Affairs Advisory Report: Privacy Amendment (Private Sector) Bill, 2000.
2. Mulligan E. Confidentiality in health records: Evidence of Current Performance from a Population Survey in South Australia. Med J Aust 2001; 174:637–640.
3. Princeton Survey Research Associates. Medical Privacy and Confidentiality Survey. Sacramento: California Healthcare Foundation, 1999.
4. Health Information and the Privacy Act 1988: A short guide for the private health sector. Sydney: Office of the Federal Privacy Commissioner, 2001.

AFP