COMMENTARY

The effect of the proposed national data protection regime on the health sector in Australia

Margaret Jackson

Margaret Jackson is Associate Professor in Computer Law, Royal Melbourne Institute of Technology, Business.

Abstract

The Commonwealth Government and a number of State governments are proposing to introduce legislation based on the Information Privacy Principles contained in the Privacy Act 1988 *(Cwlth). This will allow individuals access to any personal information held on them by any organisation or person, including private practitioners, private health facilities and State government agencies. This article discusses this proposed legislation and its implications for the health sector.*

Although in the public health area patients can already gain access to their medical records through the use of the various Freedom of Information Acts and, in the case of Commonwealth government agencies, the Privacy Act 1988 *(Cwlth), the proposed data protection legislation will provide more than access rights to individuals. The effect of the proposed legislation on the private sector, where no obligation exists on the part of the doctor to grant a patient access to his or her records, will be substantial.*

Introduction

Public concerns about personal information in the health sector include the confidentiality of that information, its use and disclosure, and access to it. All these concerns are addressed in some way by the proposed data protection legislation being considered by the Commonwealth Government and a number

of State governments. This paper explains the existing law in relation to allowing patients access to their medical records and discusses the implications of the *Privacy Act 1988* (Cwlth) being extended to cover the health sector. It examines the development of privacy or data protection legislation in Australia, the Information Privacy Principles (IPPs) contained in the Act which establish the guidelines to be followed by holders of personal information, and the proposals of various governments to extend the operation of the IPPs to the private sector and to State government agencies.

The existing law

In the health sector, it has been a long-established legal principle that a patient is not entitled to access to their medical records. This principle was tested in respect of the private sector in the case of *Breen v Williams* (1996) 70 ALJR 772, which examined whether or not a patient has the right to access to their medical records held by a private practitioner. In 1993 Ms Breen became involved in a class action in the United States in relation to a claim about defective breast implants. Her solicitor wrote to Dr Williams, who had treated Ms Breen in 1978 but who had not performed the bilateral augmentation mammoplasty operation involving the insertion of silicone implants, asking if he would forward copies of medical records concerning Ms Breen. Dr Williams advised that he would only release the records if Ms Breen would supply him with a document releasing him from any claim that may arise from his treatment of her. Ms Breen refused and commenced legal action against Dr Williams to gain access to the medical records. Subsequently, Dr Williams offered to provide Ms Breen with a summary of the contents of the records but this offer was rejected. It should be noted that Ms Breen was not claiming that she owned the medical records, the documents themselves, only the right to examine the contents.

There were three main grounds on which her claim were based. First, she had 'a proprietary right and interest' in the records. Second, the common law implied a term in the contract between her and Dr Williams to the effect that she had a legal right of access to the records. Third, the law imposed on Dr Williams a fiduciary duty to give Ms Breen access to her medical records. In support of these grounds, the appellant claimed that the common law recognised that a patient had a right to know all necessary information about their treatment, which included access to all records.

The position of Dr Williams was that, while patients may have a right to be informed of all relevant factual information contained in their medical records, they did not have a right to examine those records or have a copy of them. Such a position is in accordance with the views of the Australian Medical Association.

The court held that Ms Breen did not possess a right to access to the documents. While a contract did exist between a patient and a doctor, the court could not agree that an implied term of that contract was to allow the patient access to their records. What was implied was that the doctor must act to provide diagnosis, advice and treatment in the best interests of the patient. The decision to release information contained in the patient's medical record was for the doctor to make.

Related to the argument of an implied term to provide access to medical records, Ms Breen had argued that, as a result of the case of *Rogers v Whitaker* (1992) 175 CLR 479, patients in Australia had a greater 'right to know' about their treatment. Gaudron and McHugh JJ (at 794) disagreed that the case gave patients a right of self-determination. *Rogers v Whitaker* 'took away from the medical profession...the right to determine, in proceedings for negligence, what amounts to acceptable medical standards' but did not go further.

The court also dismissed the arguments that a fiduciary relationship existed between a patient and doctor which would entail providing access to medical records and that the common law granted a general right of access. In their joint judgment, Gaudron and McHugh JJ (at 794) conceded that some in the community might think it unfair that a patient should not be given access to their records. It was not the role of the court, however, to invent new legal rules and principles. If any change to the existing law was to be made, it must be made by the legislature.

In the public sector, legislation was enacted in the 1980s and 1990s to allow individuals and organisations access to information held by government agencies. The Freedom of Information Acts, enacted in every Australian jurisdiction except the Northern Territory, allow patients or their legally recognised representatives to obtain access to their medical records upon written request. The legislation does allow the holder of the medical records, however, to deny a request for access where the disclosure of information of a medical or psychiatric nature may adversely affect the physical or mental health of the person requesting access.

The *Privacy Act 1988* (Cwlth) also provides individuals with the right to gain access to information about themselves as well as the right to correct it. It established guidelines to be followed by collectors of information about how the information should be collected, used and kept secure. The scope of this Act has, however, been very limited.

A number of reports examining the operation of the Privacy Act have been issued by Commonwealth government committees since 1991. All recommend widening the scope of the Privacy Act so that a national privacy code can be developed. Two such reports were the discussion paper, *Freedom of Information,* released by the Australian Law Reform Commission and the Administrative

Review Council in May 1995, and the final report, *Open Government: A Review of the Federal Freedom of Information Act 1982,* released in December 1995. The discussion paper considered that 'people should have access to their personal medical records whether they are held in the private or public sector'. It could not see that extending the Privacy Act to the private sector would 'place undue hardship on private medical practitioners' (p 127). It went on to recommend that all the IPPs should apply to the health and medical area, particularly to ensure that records were protected against unauthorised use by third persons. One example of such potential misuse was that 'many commercial clinics, such as those that provide paternity tests, hold large amounts of personal medical information which, if misused, could be very damaging to the patient' (p 127).

In September 1996 the Commonwealth Government proposed that the operation of the *Privacy Act 1988* (Cwlth) should be extended to cover the private sector, State and Territory government agencies, and government business enterprises. Such an extension would have the effect of allowing individuals to gain access to and amend any personal information held about them by any person or organisation in any of those sectors, and to be notified of the existence of any records held about them.

Implications for the health sector of the extension of the Privacy Act

The Privacy Act contains 11 IPPs which operate as a set of guidelines to be followed by any person or organisation holding personal information about individuals. It is these guidelines or IPPs which will be used, albeit with some slight amendment, to apply to the health sector. The content of the IPPs is discussed in more detail below. The extension of the IPPs, by either the Commonwealth Government or a State government, to the private sector and to State government agencies will obviously allow patients access to their medical records. It is likely that the private health sector will be affected by this right the most, given the existing law as confirmed in *Breen v Williams*. The right of access granted under the Act is greater, however, than just access to medical records. The IPPs grant the right of access to any information in which an individual can be identified. That means that access can be gained to documents such as incident reports, treatment charts, reports for insurance companies, specialist reports, financial reports, and internal reports investigating a complaint, for instance, if they contain any information which may identify an individual. It is also important to be aware that the IPPs apply equally to information stored manually or on a computer.

The IPPs would, however, affect more than just access to any personal information, including medical records, which identified an individual. The public sector should note in particular that the role and purpose of the Privacy Act is different from that of the Freedom of Information Acts. The former seeks to assure individuals that, if information about them is collected and stored, it will not be misused and that they, the subjects of the information, will have some control over its use and accuracy. The latter seeks to provide a limited form of open government decision-making. The IPPs in the Privacy Act which will be of particular relevance to the health sector will be the requirement for record-holders to protect personal information by reasonable security measures (Principle 4); the requirement for a record-keeper to take reasonable steps to enable individuals to know if any personal information about them is held (Principle 5); and the restrictions which are placed on the disclosure of personal information by a record-keeper which is made without the consent of the data subject (Principles 10 and 11).

The issue of patient consent to disclosure of information was discussed in the 1995 report, *In Confidence: A Report on the Protection of Confidential Personal and Commercial Information held by the Commonwealth,* released by the Commonwealth House of Representatives Standing Committee on Legal and Constitutional Affairs. In examining the problems of access to medical records for statistical and research purposes, it highlighted as a particular concern the role of the Australian Institute of Health and Welfare in maintaining the National Cancer Registry and the National Death Index (pp 153–60). Cancer patients were generally not aware that details of their medical condition might be sent to the Australian Institute of Health and Welfare and released to external researchers. The report recommended that individuals should be notified by either the hospital admissions department or the general practitioner, both verbally and in writing, that their personal information would be disclosed to others, and the purpose of this disclosure (p 158). Such a recommendation was consistent with the requirement in the Act to notify individuals about how their information may be used and would probably satisfy the requirement not to disclose information without the individual's consent unless they had prior warning of its likely disclosure.

Health agencies will need to review admission forms to ensure collection of data is necessary, including questions relating to religion and marital status, and to ensure that information collected for the purposes of treatment is not used for other purposes by, say, the finance department (Principles 10 and 11). It will be extremely important also to advise patients when information about them which has been collected informally, perhaps in conversation, has been recorded.

There is a likelihood that the Privacy Commissioner will issue a code of practice for the health sector, as has been the case in New Zealand. The New Zealand Privacy Commissioner issued a Health Information Privacy Code which has slightly modified the New Zealand IPPs to meet the particular needs and concerns of the health sector, including the specific needs of parents, minors, next-of-kin, and those with a mental disability.

The development of data protection legislation in Australia

The issue of access to medical records is linked to the area of privacy and the right to control access to personal information held about oneself generally. In Australia, the common law does not contain a legal right to privacy although it does recognise some individual rights, such as the right not to be physically threatened (assault and battery) and the right to protect property (trespass). The case of *Victoria Park Racing and Recreation Grounds Co. Ltd v Taylor* (1937) 58 CLR 479 is recognised as authority that Australian law does not contain a general right of privacy.

Concerns over privacy can be divided loosely into two categories: concern over protection of individual personality as illustrated by invasions of privacy by the media; and concern over control of and access to information about an individual. This latter concern rose to greater prominence in the 1960s onwards as a result of developments in computer technology and the growth of government-owned data banks.

In Australia, the only legal redress available to an aggrieved individual whose personal information had been misused in some way was in contract (assuming that that person had entered an agreement with the holder of the information), in tort, on grounds of negligence or defamation; and in equity, for breach of confidence (assuming that a confidential relationship existed between the holder of the information and the confider of the information). None of these actions was entirely satisfactory. In particular, they did not allow the information subject access to the information being stored about them so as to check accuracy, and nor did they provide any redress against a person who gained access to this personal information without authority. None recognised a right to individual privacy.

During the 1970s and 1980s there were a number of attempts by various Australian governments, both Commonwealth and State, to address or investigate concerns about privacy, particularly information privacy. The approach which was finally adopted at the federal level on the recommendation of the Australian Law Reform Commission was based on the international

regulatory framework contained in the 1980 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the OECD guidelines). Arising primarily from a need to ensure that the free flow of information across borders was not halted or hindered by national laws, the OECD guidelines establish standards by which governments, organisations and individuals can collect and use personal data.

The *Privacy Act 1988* (Cwlth), which adopted the OECD guidelines after minor amendment, was passed in December 1988 and commenced on 1 January 1989. It was accompanied by legislation introducing a diluted form of the Australia Card – the tax file number scheme. Although the Australian Law Reform Commission had also recommended that the legislation should apply to both public and private sectors, the Commonwealth Government had argued that it did not consider it had the constitutional power to extend the operation of the Act beyond the Commonwealth public sector, other than in respect of the handling of tax file numbers by employers (Hughes 1991; Ross 1995).

The Privacy Act contained 11 IPPs, which are discussed in the next section, and established the position of Privacy Commissioner to act as the watchdog on breaches of the IPPs. The Act applies to information collected, stored, analysed and disseminated by any means, not just by computer technology. It requires the tax file numbers of individuals to be handled in accordance with the IPPs, whether kept by public or private sector employers, but otherwise applies only to personal information held by Commonwealth government agencies.

In 1990 the operation of the Privacy Act was extended to cover another segment of the private sector using the corporations power and banking power under s. 51(xx) and s. 51(xiii) respectively of the Constitution. The *Privacy Amendment Act 1990* specifically applied the IPPs to the activities of credit reporting agencies and credit providers.

Under the Act, the Privacy Commissioner is empowered to issue guidelines and codes of conduct in respect of areas in which they perceive interferences have arisen or may arise. The Commissioner has issued two guidelines specifically related to the health area: the *Guidelines for the Protection of Privacy in the Conduct of Medical Research 1995,* prepared in cooperation with the National Health and Medical Research Council; and the voluntary *HIV/AIDS and Privacy Guidelines,* released in 1992. Under the *National Health Act 1953* (Cwlth), the Commissioner was also empowered to produce the *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines 1994*.

The Information Privacy Principles in the Act

The purpose of the 11 IPPs in the Privacy Act is to provide guidelines on how to collect, use and store personal information about individuals. In s. 6, the Act defines 'personal information' as:

> *...information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

A record can include '(a) a document, (b) a database, however kept, or (c) a photograph or other pictorial representation of a person'. Information contained in 'a generally available publication' such as a magazine, book, newspaper or similar publication is excluded from the meaning of record. Information collected and held by an individual principally in relation to the individual's household or personal affairs would also be excluded. Clearly, a medical record would be deemed to contain personal information about an individual.

The IPPs are as follows:

Principle 1 – Manner and purpose of collection of personal protection
This principle states that personal information must be collected for a lawful purpose directly related to and necessary to the function or activity of the collector. It may not be collected by unlawful or unfair means.

Principle 2 – Solicitation of personal information from individual concerned
This principle states that when a collector collects information from the individual concerned, or the data subject, the collector must takes steps before the information is collected, or as soon as practicable thereafter, to advise the data subject of the purpose for which the data is being collected, and the names of any person or body to which this information may be passed normally.

Principle 3 – Solicitation of personal information generally
Principle 3 requires the collector to take reasonable steps to ensure the relevance, completeness and currency of the information collected and that the data collection does not intrude unnecessarily on the personal affairs of the individual concerned. Note that Principles 1–3 only relate to the collection of information by a collector and do not apply where personal information is passed on passively by an agency and where no steps were taken to obtain the information.

Principle 4 – Storage and security of personal information
This principle states how the person or body holding the personal information or controlling it, the record-keeper, must look after that information. They are

expected to protect the information by reasonable security safeguards against loss, unauthorised access, use, modification or disclosure, and against other misuse. If the record-keeper is required to give the information to another in connection with the provision of a service to the record-keeper, then the record-keeper must do everything reasonably within their power to prevent unauthorised use or disclosure of the information.

Principle 5 – Information relating to records kept by a record-keeper

Principle Five requires a record-keeper to take reasonable steps to enable individuals to know if any personal information about them is held by the record-keeper. The individual is entitled to know the nature of the information, the main purposes for which the information is used, and the steps they need to take to obtain access to the information. Record-keepers can only refuse to provide this information if another statute, such as the *Freedom of Information Act 1982* (Cwlth), permits them to refuse access to the information.

The principle also requires record-keepers to maintain a list describing the types of personal information held by them, the purpose for which each type is held, the lifetime of the record and details about access. This list is to be available for inspection by members of the public and a copy must be provided annually to the Privacy Commissioner.

Principle 6 – Access to records containing personal information

Principle 6 grants an individual the right to gain access to any personal information about them held by a record-keeper, except where the record-keeper is required by law to refuse access. It should be noted that the Act does not define the word 'access'. Chambers 20th Century Dictionary defines it *inter alia* as 'to locate and retrieve information'.

Principle 7 – Alteration of records containing personal information

This principle requires a record-keeper to take any steps necessary, including making corrections, deletions and additions, to maintain the accuracy of the information held and to ensure it is relevant, up-to-date, complete and not misleading. It also grants an individual the power to insist on a statement containing the necessary correction to be attached to the information held if the record-keeper is not willing to amend the information.

Principle 8 – Record-keeper to check accuracy

Principle 8 requires a record-keeper who has possession of information to take reasonable steps to ensure that information which is proposed to be used, having regard for the purpose for which the information is to be used, is accurate, up-to-date and complete.

Principle 9 – Personal information only to be used for relevant purposes
Principle 9 states that a record-keeper who has possession or control of information shall not use that information except for a purpose for which the information is relevant.

Principle 10 – Limits on use of personal information
This principle states that a record-keeper shall not use personal information obtained for one purpose for any other purpose unless with the consent of the data subject. Other exceptions to this guideline include cases where the record-keeper reasonably believes that it will prevent or lessen a serious and imminent threat to the life or health of the data subject or another individual, where use of the information is required or authorised by law or for enforcement of a law, or where the alternate use is directly related to the purpose for which the information was obtained.

Principle 11 – Limits on disclosure of personal information
This principle imposes a duty on a record-keeper not to disclose personal information to a person or organisation, other than the data subject, unless the data subject should reasonably have been aware, or was made aware under Principle 2, that information of this kind was normally passed to that individual or organisation; unless the data subject has consented; unless disclosure is required by law; or unless the record-keeper reasonably believes that the disclosure will prevent or lessen a serious and imminent threat to the life or health of the data subject or another individual.

Proposed national privacy protection regime

In September 1996 the Federal Attorney-General, Daryl Williams, released a discussion paper, *Privacy Protection in the Private Sector*. The approach to extending data protection to the private sector and to State government agencies discussed in the paper is a co-regulatory one, providing for, as a key component, the development and adoption of codes of practice based on a set of IPPs.

The proposed data protection regime would apply IPPs based on, but not necessarily identical to, those contained in the *Privacy Act 1988* (Cwlth) to records containing personal information. Even if no personal information was involved, the Attorney-General sees a role for the Privacy Commissioner in issuing guidelines in situations where the privacy of an individual might be adversely affected, such as telemarketing and optical surveillance.

The government envisages that the new regime would apply to all individuals and organisations in Australia, including Commonwealth government business

enterprises, such as the Telstra Corporation and Australia Post. The activities of the media are excluded from the present proposal; however, the paper states that separate consideration will be given to this area.

As mentioned above, the IPPs to be used in the industry codes of practice are to encompass 'all the internationally recognised tenets of privacy protection' and are to be based on the IPPs contained in the Privacy Act (p 6). The paper mentions that the latter will form the basis of the private sector IPPs but, with one exception, does not discuss ways in which the new IPPs may differ from the current ones.

The one amendment to the IPPs which is specifically described is that an additional IPP will be included to provide 'that an individual or organisation is not to keep personal information for longer than is required for the purposes for which the information may lawfully be used' (p 12).

As part of the proposed regime, codes of practice are able to be developed to cover specific industry groups or activities. The IPPs must be accepted as a minimum standard by each code, although some modification of the principles is to be permitted. Either the Privacy Commissioner or a specific private industry group may develop codes of practice, but any industry-generated codes must be approved by the Commissioner. Codes will not be able to limit or restrict an individual's access to and right to correct information held about them. If no code is issued, the IPPs will apply.

The Privacy Commissioner is to be granted responsibility to oversee compliance of the private sector with the IPPs and their role is to be widened to allow this to occur. New functions to be undertaken by the Commissioner include the right to issue codes of practice, to monitor and report on security safeguards to protect personal information, to make public statements in relation to privacy matters, and to investigate activities which, although not a breach of an IPP *per se*, may affect the privacy of individuals. Some of the new functions appear quite broad and will result in the Commissioner being granted power to investigate all privacy issues, not just those that relate to information privacy. While the Privacy Act currently empowers the Commissioner to act in cases which involve 'interferences with privacy', it narrowly defines an 'interference with privacy' as referring only to a breach of one of the IPPs. It is clear that the Commonwealth intends the Commissioner to take a broader role in protecting the privacy of individuals, even beyond the extension of the IPPs to the private sector, but the exact nature of the role will need further clarification.

Organisations will be required to appoint an employee as their privacy officer, although this role does not have to be the sole function of such an officer. No

individual liability for breaches of IPPs by the organisation will be borne by the privacy officer, although organisations and individuals will be liable for the acts of employees which may result in a breach. The new regime will also introduce penalties for the unauthorised disclosure of personal information for profit and for obtaining personal information by false pretences. There are no penalties suggested for those individuals and organisations who procure the unauthorised release of personal information, although such penalties were strongly recommended by the Privacy Commissioner, and by two important reports, the 1995 *In Confidence: A Report on the Protection of Confidential Personal and Commercial Information held by the Commonwealth* (Commonwealth House of Representatives Standing Committee on Legal and Constitutional Affairs) and the 1992 *Report on Unauthorised Release of Government Information* by the New South Wales Independent Commission against Corruption. This is a noticeable gap in the proposed regime which other countries, such as the United Kingdom and Austria, have handled within their data protection legislation.

The new data protection regime also addresses the issue of transborder data flows. The transfer of personal information out of Australia to countries with inadequate levels of privacy protection will only be permitted where a number of requirements are met. These requirements include if the individual concerned had consented, if the transfer was necessary for the performance of a contract between the individual and the record-keeper; if the record-keeper believed on reasonable grounds that the disclosure was necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person; if the disclosure was required or authorised by or under law; or if the record-keeper had in place adequate contractual safeguards to protect the privacy of the information.

The Attorney-General has stressed that the government wants the development of private sector data protection rules to be a consultative process with industry and that it views the release of the discussion paper as a first stage. After consideration of submissions relating to the paper, draft legislation should be introduced in 1997.

State and Territory government initiatives

As well as the proposal from the Commonwealth Attorney-General for a national data protection regime, a number of State and Territory governments have acted or are proposing to act to enact data protection measures in some form.

1. Victoria

In August 1996 the Victorian Government established a Data Protection Advisory Council to advise on appropriate draft legislation for data protection. The main incentive for the creation of the council was acknowledged by the Victorian Treasurer and Minister for Multimedia, Alan Stockdale, to be the introduction of a government database, the Electronic Service Delivery.

The terms of reference for the Data Protection Advisory Council require it to advise the Minister for Multimedia on the 'most appropriate regulatory regime for Victoria governing collection, storage and transfer of information, particularly personal information held by the public sector organisations' (Victorian Government Press Release 1996, p 1). The primary focus of the council, therefore, is to be on the public sector, but it is not restricted to personal information only. It is required to consider other data protection and privacy regulation models, principles and experience in other jurisdictions, and to consider the desirability of regulation of the private sector in view of the potential Commonwealth government activity in this area.

The council was due to report to the Minister by 20 December 1996 on its recommended data protection regime, including draft legislation if appropriate. It is expected that its recommendations will only apply to the public sector.

2. New South Wales

New South Wales has had a Privacy Committee since 1975. Its role is to monitor privacy concerns, to conduct research into the development of a general legislative philosophy for privacy, to recommend appropriate legislation, to encourage the development of codes of conduct for business, and to investigate individual complaints of infringement of privacy. Although hampered by a lack of power to sanction those who interfere with the privacy of others, the committee has actively investigated complaints from the public and recommended ways in which privacy can be protected. It has released a number of usefuls reports on aspects of privacy protection, including its 1986 *Guidelines for the Operation of Personal Data Systems.*

In 1991 a private member's Bill, the Data Protection Bill, was introduced by Mr Andrew Tink into the New South Wales Parliament. Debate on the Bill was deferred, however, pending an investigation being conducted by the New South Wales Independent Commission Against Corruption.

In 1990 the Independent Commission Against Corruption had become aware that a private inquiry agent had gained access to confidential government information without authority. Concerned that this breach could be part of a

wider trade in government records, the commission commenced a two-year inquiry. It found that a flourishing trade in government information existed at both State and Commonwealth level, involving the public and private sectors. It also found that the existing criminal law in New South Wales was inadequate to handle the abuses uncovered. The final report titled *Report on Unauthorised Release of Government Information*, released in August 1992, found that a total of 155 people had engaged in corrupt conduct and a further 101 had engaged in conduct which allowed, encouraged or caused the occurrence of corrupt conduct. One of its recommendations was that uniform data protection laws should be introduced throughout Australia.

After the release of the Independent Commission Against Corruption Report, the Attorney-General, Mr John Hannaford, indicated that he would introduce data protection legislation as soon as possible (New South Wales Privacy Committee 1991, p 2). It was not until March 1994, however, that an amended Privacy and Data Protection Bill was released. No further action on the Bill occurred and the government subsequently lost power.

The new Attorney-General, Geoff Shaw, has stated, however, that he will proceed with a new Privacy and Data Protection Bill, covering both the private and public sectors, before the end of 1996.

3. Australian Capital Territory

On July 1 1994 the Privacy Act was amended to cover agencies of the Australian Capital Territory, pending the introduction of privacy legislation in the Territory.

4. South Australia

Although South Australia created a Privacy Committee in 1983, its approach to data protection has differed from that of New South Wales and Queensland. In 1989, by means of Cabinet Administrative instructions, a set of IPPs were adopted for application to the collection, storage and use of personal information by the South Australian public sector. Individuals are able to examine any personal information about themselves. The Privacy Committee is able to investigate the compliance of State government agencies with the IPPs (Legal & Constitutional Committee 1990, p 41).

5. Western Australia

Western Australia had no specific privacy legislation. A private member's Bill, the Data Protection Bill, was introduced into Parliament in 1988 and reintroduced in 1989, but did not proceed. Since that time, various governments had indicated they would introduce some form of privacy legislation.

In August 1995 the Commission on Government, established to inquire into matters relating to corrupt, illegal or improper conduct of government officials, released its first report. Privacy protection was one matter examined. The commission decided to focus only on the privacy issues surrounding 'the storage, use and retrieval of personal data and the exchange of data between government agencies' (p 61). It recommended, *inter alia*, that privacy legislation should be enacted to address specific privacy issues surrounding the storage, use and retrieval of personal data and data matching between government agencies. This legislative scheme should be based upon IPPs modelled upon those in the *Privacy Act 1988* (Cwlth) and should apply to the public sector and to private sector contractors performing government work. A Privacy Committee should also be established.

As a result of the commission's recommendation, the Western Australian Attorney-General requested the Ministry of Justice Department to prepare an options paper for privacy legislation in the State.

6. Northern Territory

In mid-1996 the Northern Territory Attorney-General asked the Secretary of his Department and the Anti-Discrimination Commissioner to prepare an options paper on privacy to place before Cabinet (Greenleaf 1996, p 100).

7. Queensland

Queensland also established a Privacy Committee in 1984, with similar functions to the New South Wales Privacy Committee. In 1992, however, the Privacy Committee was wound up when the sunset clause in the *Privacy Committee Act 1984* (Qld) took effect. At the end of 1995 a Queensland interdepartmental committee was set up to investigate how to implement a proposal to adopt the Privacy Act IPPs in the Queensland government sector and to look at the option of a statutory privacy law (Greenleaf 1995, p 140). In early 1996, however, the then Labor Government lost power.

The current government has indicated that, while data protection legislation is not a priority, it will introduce some form of data protection controls for the public sector in 1997, possibly along the lines of the South Australian administrative guidelines.

Conclusion

By the end of the century, Australia will have data protection legislation which covers the private sector, government business enterprises, as well as State and Territory government agencies. This coverage will be achieved by a widening of the application of the Privacy Act and, possibly, by the introduction of various State Acts. The IPPs contained in the Privacy Act will provide the basis for this national comprehensive data protection scheme. The full implications of this new legislation for the health sector will not be clear until after it is enacted, but it will be substantial in its effect on patient rights to gain access to information and on the responsibilities of the health sector in terms of collecting, protecting, using and disclosing personal information.

References

Australian Law Reform Commission & the Administrative Review Council 1995, *Freedom of information*, Discussion paper, Australian Government Publishing Service, Canberra, May.

Australian Law Reform Commission & the Administrative Review Council 1995, *Open government: A review of the federal Freedom of Information Act 1982*, Final report, December, Australian Government Publishing Service, Canberra.

Chambers 20th Century Dictionary 1983 edition.

Commonwealth House of Representatives Standing Committee on Legal and Constitutional Affairs 1995, *In confidence: A report on the protection of confidential personal and commercial information held by the Commonwealth*, Australian Government Publishing Service, Canberra.

Federal Attorney-General, Daryl Williams, 1996, *Privacy protection in the private sector*, Discussion paper, September.

Greenleaf G (ed) 1995, 'Private parts: Qld joins privacy push', *Privacy Law & Policy Reporter*, vol 2, no 7, p 140.

Greenleaf G (ed) 1996, 'Private parts: Territorial privacy', *Privacy Law & Policy Reporter,* vol 3, no 5, p 100.

Hughes G 1991, *Data protection in Australia*, Law Book Co, Sydney, pp 68–103.

Legal & Constitutional Committee 1990, *Report upon privacy and breach of confidence,* Victorian Government, Melbourne, 41.

New South Wales Independent Commission Against Corruption 1992, *Report on unauthorised release of government information*, ICAC, Sydney.

New South Wales Privacy Committee 1986, *Guidelines for the operation of personal data systems,* Privacy Committee, Sydney.

New South Wales Privacy Committee 1991, *1991 Annual Report*, 2, Privacy Committee, Sydney.

OECD 1980, *Guidelines governing the protection of privacy and transborder flows of personal data,* OECD, Paris.

Ross G 1995, 'The law of information privacy in Australia – A review of federal legislative protection in light of common law deficiencies', Unpublished minor thesis for Master of Laws, University of Melbourne, pp 73–6.

Victorian Government (Alan Stockdale; Minister for Multimedia) Press Release, 3 August 1996, 'Data Protection Advisory Council', Victorian Government, Melbourne.

Western Australia, Commission on Government 1995, *Report No 1*, 2, August, Western Australian Government, Perth.

Australian Health Review sought the following replies to the commentary, 'The effect of the proposed national data protection regime on the health sector in Australia', by Margaret Jackson.

Being out of step is sometimes desirable

ANTHONY R MOORE

Anthony Moore is Director of Clinical Services, Aged Care and Rehabilitation, The Mount Eliza Centre.

'Our strengths are our weaknesses, our weaknesses are our strengths,' is what he said, or something like that. I can't remember exactly. My mind was still unsettled by something the lecturer had said a little earlier.

'Lateral thinking is too limited,' he said. 'It's only in one direction, and usually in the opposite direction to that which you have been thinking. What we need is spherical thinking! In all directions, and for an infinite duration.'

What bothered me was a drawing he placed on the whiteboard. A neat circle representative of the sphere. He asked the audience what it was. The usual answers of a ball, a balloon, the moon, were offered.

'Actually,' he said. 'It's a picture of a profound icon.'

We all looked appropriately puzzled. He explained:

'What is in the circle is finite, what is outside is infinite.'

There was a pause.

'What is inside the circle is your current job, outside the tens of thousands of job possibilities you have passed over. What is inside is the partner you have selected, what is outside are the few billion people on the planet who have avoided that opportunity. What is inside is the place where you live, and outside the almost infinite locations you have chosen not to. Of greater importance, what is inside is the opinion, truth and belief you hold, and the perceptions on which

they are based, and outside all the opinions, truths, and beliefs you have neglected, together with the views and perceptions you have ignored.'

What has all this to do with Margaret Jackson's article. As Associate Professor in Computer Law, one could expect that her perspective would be from this position. Indeed, that is the strength – and the weakness – of the article. The title is tantalising. We are promised an excursion into 'The effect of the proposed national data protection regime on the health sector in Australia'. Yet only 10 per cent of the article actually deals with the effects. It feels a little as though we have been promised a meal, but offered a menu.

Understandably, the article has a legal emphasis and perspective. There is no mention of patient surveys, public opinion, or professional opinion within the health sector, on the issues raised.

The law is not the ultimate warrant of human conduct, nor is the law the most important arbiter of human belief or behaviour.

Over 90 per cent of the article is an account of various legal principles – as illustrated by precedent in the courts – legislation at a Commonwealth and State level, Information Privacy Principles (IPPs) in the Privacy Act, codes of practice, and State and Territory government initiatives.

Practitioners in the health sector reading the article, while noting the implications of privacy legislation in relation to banking, tax, telemarketing, optical surveillance, Telstra, Australia Post, corruption inquiries, and improper conduct of government officers with interest, may feel that a more detailed and practical consideration of the implications of such legislation, inquiries and codes on *clinical practice* would have been more helpful.

The paper is most informative in outlining the 11 IPPs, and drawing on them strongly in the section 'on the effects on the health sector'.

The paper notes, firstly, that what has applied in the public sector for some time, now will be on the shoulders of the private health sector as well.

Secondly, it indicates that access to information under the proposed national data protection regime will involve more than medical records, and mentions incident reports, therapy charts, specialist reports, and reports to insurance companies as some of these issues. Practitioners may be surprised to see these items in a list of documents beyond the boundaries of the medical record, as in most organisations these items are filed in the medical record.

The article also mentions patient information on computer being subject to the same principles.

The article is strongest when analysing how each of the IPPs will affect the health sector: for example, Principle 4, the obligation to protect information; Principle 5, involving the obligation to inform individuals on the information stored about them; Principles 10 and 11, outlining the restrictions on disclosure; and Principles 2 and 10, on the obligation to review data focus and the information necessary.

The article is at its most candid in admitting that the implications of both the legislation and the IPPs are not yet clear, because new practices/legislation have not yet been fully established.

Even when they are, there will still be difficulties. The passage of a law or a regulation does not resolve a personal dilemma at the heart of an ethical conflict. Indeed, ethics is the study of the way we react to moral dilemma. Such dilemmas are not resolved by the passage of a law. The law is simply one ingredient in the ethical milieu in which an individual will make a decision. What the law does is define what is legal or illegal.

And there's the rub. A patient's medical file is not a legal document. It is a clinical document. It has not been written with 'one eye over the shoulder' in the fear that one day the record may appear in a court of law, or be the subject of evidence in litigation. It has been written in order to document clinical events and clinical items, so as to improve and ensure the highest patient care, and information exchange between the health caring professionals caring for that patient. If legal issues begin to dominate the approach to a professional writing in the medical record to the detriment of patient care, few, except lawyers, will benefit.

There are other concerns:

1. Patient documentation may contain copies of correspondence from other health professionals and organisations who may have referred the patient to the current service or practitioner. Release of such information, without culling, could expose other practitioners to what was considered confidential information being released without their knowledge. This is particularly important in relation to psychological, psychiatric and neuropsychological reports, but also in relation to social work and details of a referring practitioner's involvement with that patient.

2. A patient's medical file may contain information about family members, partners and other contacts. The release of this information in an unfiltered way could cause grave concern to individuals not primarily the focus of a medical record. This is particularly so in relation to social work reports. Any thorough

medical history would have detailed information on the family and the community support structure involved with that patient.

3. That patient's opinions about other practitioners may also appear in a medical file, and it would be clearly inappropriate for this indirect source of opinion to be accessible without safeguards.

The critical issue in all of this is the point made above. A patient's medical record is a clinical document which may, on occasions, have legal implications. The issue of privacy is fundamental, and confidentiality is a basic objective in medical practice, extending back even before the Hippocratic Oath, which embodied clauses on the importance of confidentiality.

Complex issues are not made simple by the passage of laws which fail to take into consideration the nuances of human behaviour, human preference, eccentricity, oddity, bias, prejudice and whimsicality.

Human nature dances: medical science walks; and the law marches. Sometimes being out of step is not only unavoidable, it is desirable.

Privacy versus the collective good

Judith Dwyer

Judith Dwyer is Chief Executive Officer, Flinders Medical Centre, and Board Member, Australian Institute of Health and Welfare.

Associate Professor Margaret Jackson presents a coherent analysis of the potential impacts of proposed information privacy legislation on the private and public sectors of the health system. She points out that this is not just about access to records (something the public sector has been living with for a long time, in most States) but also may bring new obligations and restrictions in the areas of how records are protected, who has access to them, for what purposes they are used and how they are updated.

While the thought of yet more regulation of our overburdened industry will not gladden many hearts, it is important to remember that, for most of the time, the patient and health care provider are working together in a relationship of trust. Our efforts to protect the rights and interests of both parties, particularly

when things go wrong, and indeed to minimise the chances of things going wrong, need to be designed not to interfere with this important reality.

In the public sector, patient access to medical records under freedom of information brings real costs in time and paperwork, but has not compromised the provision of care or the provider–patient relationship. Many would argue that things are better, and that the tone of correspondence and records has been improved by the knowledge that they may be read by their subjects.

Jackson gives a clear explanation of the potential impacts of other aspects of the Information Privacy Principles (IPPs). In my possibly optimistic assessment of our current practice, it seems that public hospitals are already complying with, for example, requirements for safeguarding information (Principle 4), collecting the information by lawful and fair means (Principle 1), and enabling people to know if we hold information about them (Principle 5). Principles 9 (personal information only to be used for relevant purposes) and 10 (limits on the use of personal information) may raise some issues – is it still okay to use past patients' names and addresses to solicit donations?

In assessing the implications, Margaret Jackson notes that potentially access can be gained to any record containing personal information, not just case notes. This will require a re-examination of the various ways in which privilege is accorded to, for example, information collected for quality management activities, and it may require change in the way we collect and record information from some other internal processes, including complaints investigations. From a practical point of view, this seems to me to be largely a useless exercise in the end (we will, one way or another, have to be able to have privileged conversations about problems), but it looks likely to happen.

Whatever the details turn out to be, it is clear that we must act effectively to protect the privacy of patients. But in all of this development of machinery to do so, there are a couple of other values which need to be given weight. While everyone values their privacy, Australian people also have a strong and honourable tradition of valuing both the collective good and participation in endeavours like health research.

The establishment of cervix screening registers exemplifies the former. In both Victoria and South Australia, consultation with women's groups was very effective in establishing support for the inevitable compromise between privacy and health concerns. Women were overwhelmingly in favour of a central register because it would assist all women to avoid cancer, even though they understood very well the implications for their privacy. And while a small number of women in South Australia have taken the 'opt out' course, there has been a remarkable

lack of concern or reaction as the letters to women's homes began arriving from the registry.

The generosity of most people who respond positively (and often with enthusiasm) to requests to participate in health research is testimony to our community's high level of willingness to balance their privacy concerns with their commitment to the common good. Clearly, informed consent is a key issue, and the community's continuing generosity will depend on good performance in this area. Associate Professor Jackson rightly points out the need for cancer patients to understand that information about them will go to cancer registries and be linked to other databases. But in designing the systems to ensure this, there should be no assumption that the people involved will value their privacy above the potential for there to be some larger good arising from their illness. Experience indicates the opposite.

It seems to me that it is vital that those with an interest in research and public health, as well as those who can directly represent the interests of the community generally and research subjects in particular, are involved in the design of the health industry code of practice, which clearly we will need to have.

Privacy and quality health care

Janne D Graham

Janne Graham is President of the Health Care Consumers' Association of the ACT and a former Chair of Consumers' Health Forum of Australia Inc. She was a consumer representative on the National Health and Medical Research Council working party which drew up the council's *General Guidelines for Medical Practitioners on Providing Information to Patients*.

Adele had been unable to work for some time and her employer's superannuation insurers were considering her application for a pension. They required a blanket consent from her for access to all her medical records. She didn't feel comfortable about this consent until she herself knew what they contained.

Bob overheard two staff members in the hospital talking about his condition and began to feel that his symptoms were not being taken seriously. He thought it would be a good idea to see what was being said 'on the record'.

Carol's baby was progressing well in neonatal intensive care. Everybody said so. Then he died during a routine procedure. Carol felt that the hospital was covering up and that something had gone wrong in the conduct of the procedure. Being a nurse herself, she could understand how it might happen. She wanted to see the records to know.

Adele, Bob and Carol, like consumers generally, want access to their records for a range of reasons, including checking their accuracy; maintaining some control over their treatments (and lives); and gaining a better understanding of their conditions and treatments. What rights do they have if their providers are in the private sector?

Margaret Jackson considers, from a legal perspective, the current circumstances in which consumers can gain access to their medical records and the specific pieces of legislation which have facilitated this. She then draws on the Commonwealth Attorney-General's discussion paper (1996) and various State proposals to explore the implications for private health providers if the Commonwealth privacy principles were extended to apply generally in the private sector.

The paper serves as an 'alert', with sufficient background about the opening up of access in the public sector to give private providers some idea about what may be ahead for them. Since the details of any legislative reform are not yet settled, particularly regarding any co-regulatory mechanisms, the organisational and practical implications cannot be detailed. It is clear, nevertheless, that application of the privacy principles will involve more than record access. It will include data collections, record-keeping and storage. I would add form design.

The risk in addressing the issue from the legal perspective alone is that readers may be left with the sense that additional burdens are to be imposed on them because of some political decisions which have little or nothing to do with them, with health care, or their professional role. The legal approach emphasises obligations. What it does not, and perhaps cannot do, is address the central issues of quality health care.

Adele, Bob and Carol want access to their records because of concerns about health care. In the current environment, consumers generally give information and providers create, maintain and hold records. When consumers feel powerless or things are perceived as having gone wrong, consumers are automatically cast into the role of 'claimant', with consequent risk of the provider becoming a 'defendant'. This is the antithesis of a good health care relationship.

Consumers want good quality health care. This entails the opportunity for active participation in their own health care, care based on accurate and reliable

information, care that is effective and efficient and based on valid and reliable research.

The National Health and Medical Research Council's (1993) *General Guidelines for Medical Practitioners on Providing Information to Patients* are a good practice starting point for all health providers, public and private, to consider their role in information provision. Providing appropriate (or as the lawyers say 'material') information requires effective listening and, by implication, accurate recording. Whilst consumer organisations are not expecting any legislation on access to records in the private sector to be retrospective, there could be no great harm in dealing with record-keeping now as though it were part of the shared relationship between providers and their patients. There is evidence (Public Interest Advocacy Centre 1996) that consumer involvement in record-taking and review contributes to improved accuracy and improved health outcomes. For instance, I believe that my identification of a pathology report wrongly on my hospital file led to the more timely treatment of another patient and I know that when I could prove to the palliative care team that their records were inaccurate (and that I was not 'in denial' about my relative's condition), unnecessary services were stopped.

Legislation which clarifies providers' responsibilities in storing, sharing, keeping and destroying records should be welcome. The current situation is unclear, varies between jurisdictions and can leave providers, consumers and families without needed information.

The aim of record transfer and record sharing is to improve care. Including consumers and sharing the information with them will contribute to both trust and improved coordination.

Health consumers have a vital interest in the outcomes of sound and relevant health research and are generally willing to have their records contributed, but we need to be satisfied about the appropriateness of the research and the reliability of the information, either personally or through accountable procedures being in place.

It is quality health care issues such as these which private providers need to be addressing as they consider the challenges of possible legal changes aimed at making health records more readily accessible and their recording storage and uses more accountable.

References

Federal Attorney-General, Daryl Williams, 1996, 'Privacy protection in the private sector', Discussion paper, September.

National Health and Medical Research Council 1993, *General guidelines for medical practitioners on providing information to patients,* Australian Government Publishing Service, Canberra.

Public Interest Advocacy Centre 1996, 'Whose health records?' October.

What will legislation achieve?

CHARLOTTA BLOMBERG

Charlotta Blomberg is Legal Counsel, Australian Medical Association.

Of all the health public policy issues, patient access to medical records is one which generates strong opinions and vigorous debate. Debate on the issues of access (by whom, to what and how) often becomes lost amid the discussion of 'rights'.

Since the High Court's finding in *Breen v Williams* that there is no right of patient access to medical records in common law, much attention has been focused on creation of a right through statute.

At present the ACT Government is drafting legislation to enable individuals to gain access to records held and created by health service providers. The release late last year of the Commonwealth Attorney-General's discussion paper on Privacy Protection in the Private Sector led some to conclude patient access to medical records would be secured through application of the Information Privacy Principles (IPPs) contained in the *Privacy Act 1988* (Cwlth). The dying hours of the last parliament saw the introduction of a legislative proposal by Senator Belinda Neal (Labor, New South Wales) whereby doctors would be required to enter into agreements with the Health Insurance Commission to enable their patients to obtain Medicare benefits. A term of any such agreement would be patient access to medical records. That proposal has been referred to the Senate Community Affairs Committee, due to report by 25 March.

In this context Jackson's article appears. It reviews existing statutory protection for personal information collected, stored and used by government, but does not question if these protections are appropriate for private medical records. Similarly, although the decision and facts of *Breen v Williams* are reported, the implications of the High Court's judgment on any statutory proposal to guarantee patient access to medical records are not examined. No mention is made of the current Australian Standard on protection of private health information. Instead, there is the statement that extension of the statutory-based Information Privacy Principles by either the Commonwealth or a State government will 'obviously allow patients access to their medical records'. A close reading of *Breen v Williams* shows that this is far from obvious.

The debate is now centring on providing patient access via the extension of Commonwealth IPPs, formulated under the Privacy Act, to the private sector through sector-based codes of practice. The Privacy Act and IPPs relate to the collection, storage and use of personal information by government. Principles 6 and 7 respectively allow individuals to gain access to personal information kept by government and to alter records containing personal information to ensure that it is accurate.

The legal issues identified by the High Court in *Breen v Williams* remain unaddressed or dismissed in most discussions, but they cannot be ignored. Similarly, the appropriateness of applying the IPPs to the private health sector is not questioned.

The IPP regime was created to protect individual privacy when governments collect, store and use data on individuals. In these circumstances the information gatherer is remote from the individual. There is little or no contact with the individual concerned. This is an entirely different situation from the giving and receiving of information in a medical treatment setting. The trend to 'contract out' many government functions has meant that the private sector now collects, stores and uses information on behalf of government and there must be some means to protect information relating to individuals.

Breen v Williams settled the common law on ownership and access to private medical records. The High Court ruled unanimously, though in separate judgments, that there is no patient right of access to medical records created by doctors in private practice; these documents are created by the treating doctor and belong to the doctor, unless they have been created on the patient's behalf pursuant an agreement to do so; the documents are literary works within the definition of the *Copyright Act 1968* (Cwlth); copyright subsists in these documents; copyright enables the doctor/author to determine who is able to deal with the work.

Any legislation allowing patient access to medical records in the private sector must address these legal issues. Any legislative proposal must therefore extinguish or modify the existing legal rights of one group in order to create rights in another. The proposal to deprive one group of authors (doctors) of rights in their intellectual property raises many questions of public policy. It also raises a fundamental question of whether or not legislation is even necessary.

A right of cooperative access already exists. It is settled Australian Medical Association policy that patients have a right to be informed of factual information contained in the medical record. On request, patients should be informed of their history, results of tests and investigations, findings on physical examination, the diagnosis or diagnoses, and any proposed plan of management. Access to any other parts of the medical record (such as reports by specialists) is at the discretion of the doctor. In addition, patients have a right of access when legal proceedings are on foot. Some jurisdictions provide for access to documents when legal proceedings are contemplated.

The question must be asked: 'Why is legislation necessary when access can be gained in consultation with the treating doctor?'

The recent annual reports of the New South Wales Health Care Complaints Commissioner (HCCC) and the Victorian Health Services Commissioner (HSC) show that there are only a small number of complaints regarding access to medical records. In New South Wales, of the 1516 complaints received by the HCCC, only 37 related to records. Under 'Number of Complaints Received and Assessed for Conciliation', the HCCC reports two related to privacy and one to access to records/reports. In Victoria the situation is similar. Of the 1736 new complaints lodged in 1995–96, 35 related to access to records, 14 to accuracy of records and 28 to confidentiality/privacy.

What will legislation achieve? Putting it simply, legislation will give patients a legally enforceable right (with some limited exemptions) to gain access to documents created in the provision of their health care. It will penalise doctors who refuse requests for access. It will introduce a system of judicial review of refusals of requests for access. It will remove clinical input from consideration of whether or not access should be granted. It will create more problems that it solves. Access is already possible. Legislation will create a cumbersome bureaucratic regime to administer what is already occurring.

Meaningful and workable legislation needed

Wayne Cahill

Wayne Cahill is a Partner with Hunt & Hunt, Sydney.

Margaret Jackson is to be commended on her very broad paper on the effect of the proposed national data protection regime on the health sector in Australia.

Jackson has sought to summarise case law and principles. Such summarising occasionally (as with all such attempts) can result in some possible misinterpretations.

It is unfortunate that in the article there is a tendency to refer to the public and private sector in relation to access to medical records. In my view there are in fact three sectors: (a) public facilities; (b) private facilities; and (c) the private provider. The case of *Breen v Williams* related to the latter group.

Access to medical records in the public sector has been common and policy in a number of States for over 20 years. For example, in the early 1970s the former New South Wales Health Commission recommended by administrative direction access to medical records. This was subsequently entrenched further with the Freedom of Information Act in that State (and in other States).

On that basis, Jackson' view that it has been a long-established legal principle that the patient is not entitled to access to their medical records is incorrect.

It is correct in relation to the private practitioner category above, but not in relation to category (a) and, arguably, category (b). In relation to category (b), in a number of States there is legislation which provides access to medical records. For example, in New South Wales it has been the legal situation since 1991.

In all jurisdictions there is not unlimited access, with safeguards against access usually on the basis of medical reasons.

The potential application of Information Privacy Principles (IPPs) on a national level and to a number of States has been on the drawing board for a number of years.

The Federal Attorney-General's September 1996 discussion paper has taken this a step further. The blanket application of the IPPs as they are currently contained in the discussion paper would have significant implications for the health sector.

It is important from the health perspective that IPPs are not introduced without due consideration. The following examples show where there may be problems from a blanket interpretation.

Principle 2 – The collector shall take steps to advise the data subject of the names of any person or body to whom the information may be passed normally. In a hospital situation, this is clearly silly.

A number of States already have protective legislation in place (often with gaol terms if there is a breach) to protect inappropriate release, for example, Section 22, *Health Administration Act 1982* (NSW). The principles of privacy and confidentiality are accepted readily in the hospital industry in my experience.

Principle 5 – Information relating to records kept by the record-keeper
This principle required the record-keeper to take reasonable steps to enable individuals to know if any personal information is held by the medical record-keeper. This includes requiring the main purpose for which information is used to be provided to the person about whom the data is collected. This would need explanation and suitable application in a hospital setting.

Principle 7 – Alteration of records
This principle may create problems in relation to information being 'relevant, up-to-date, complete and not misleading'. Bearing in mind that medical records are contemporaneous notes, the overzealous application of 'up-to-date and complete' may be difficult. This has to be acknowledged in the sense on the obligations in the health industry. Similarly, the obligation upon the health record-keeper to check accuracy in Principle 8 also must be taken into account.

There also needs to be attention paid to ensuring a close fit between Commonwealth and State laws in relation to the various regimes. What is of concern is that principles (to which many people would subscribe) may be applied which are not realistic and pragmatic in the health care setting.

Jackson notes that IPPs 2 and 10 may place an obligation to advise patients when information about them collected 'informally perhaps in conversation, has been recorded'. This would often occur in a medical record and again illustrates the need to adapt appropriate health-specific guidelines.

It is also important to be aware of the important distinction made by Jackson as to the differing role and purpose of the Privacy Act as compared with the Freedom of Information Acts. Proposals under the IPPs extend obligations to record-keepers and this will have significant implications in the health industry.

Privacy and confidentiality is an emerging legal issue of which the health industry has been cognisant for some time. The implications of the Privacy Act and the IPPs will, however, place additional pressures upon the health industry. It is incumbent upon the Australian Healthcare Association to make appropriate submissions to ensure that what is introduced is meaningful and workable and not 'over the top'.