JULIE CLAYTON, VIC

Privacy legislation and personal injury practice

This article seeks to give a brief outline of privacy legislation both at a federal level and in the state of Victoria, and looks at some of the implications for legal practice in the area of personal injury.

The Legislation

The relevant privacy legislation discussed in this article is the *Privacy Amendment (Private Sector) Act 2000* (Cth) which applies to all areas of the private sector, the *Health Records Act 2001* (Vic) which applies to "health information" in the private and public sector and the *Information Privacy Act 2000* (Vic) which applies to the public sector.

The Privacy Principles

Privacy principles are nearly identical in each of the three Acts. The Health Records Act also deals with the closure of a medical practice and the provision of health information between health services providers.

Collection

An organisation must not collect personal information unless the information is necessary for one or more of its functions and activities. The organisation that is collecting the information must take reasonable steps to ensure that the individual is aware of the purposes for which the information is collected and to whom the information will be disclosed.

For both lawyers and doctors it is generally going to be clear why the information is being collected. Lawyers should ensure that clients know that personal information may be disclosed to medico-legal experts and barristers.

Julie Clayton is a Solicitor at Slater and Gordon
PHONE 03 9602 6888 **EMAIL** jclayton@slatergordon.com

Use and Disclosure

An organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection or a directly related secondary purpose.

Data Quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Data Security

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure.

Openness

An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Under the federal legislation an organisation may develop a "privacy code" to be approved by the Federal Privacy Commissioner. Alternatively, an organisation can simply have a privacy plan. ▶

" . . . individuals must have the option of not identifying themselves when entering transactions with an organisation."

Access and Correction

If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual.

There are some exceptions to this provision, such as where providing access would have an unreasonable impact upon the privacy of other individuals or where the information relates to legal proceedings and the information would not be accessible by the process of discovery in those proceedings.

A further exception is where an enforcement body performing a lawful security function asks the organisation not to provide access on the basis that it would cause damage to the security of Australia. One would imagine that the threshold would need to be fairly high to rely on such an exception.

If an organisation holds personal information about an individual and that individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

Identifiers

An organisation must not use an identifier of an individual that has been assigned by an agency, or an agent of an agency, or a contracted service provider for a Commonwealth contract.

This would seem to be most relevant to health service providers and prohibits them from using Medicare numbers for their file identification.

Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

Trans Border Data Flows

When information is to be transferred overseas, the transferor should ensure that the recipient is also subject to privacy regulations. Under this principle, the transfer of information overseas is not allowed unless the individual consents to the transfer; or other fairly narrow criteria are met. Essentially this seems to impose a requirement that information that is transferred is done so in a way that ensures that privacy principles are maintained.

***Sensitive Information* - Privacy Amendment (Private Sector) Act 2000**

An organisation must not collect sensitive information about an individual unless the individual has consented, collection is required by law, or collection is necessary.

This principle is not included in the Health Records Act and does not apply as, by definition, health information is sensitive information.

A lot of the information lawyers collect is sensitive. Obviously the client's consent is required to obtain medical or employment records.

***Transfer or Closure of the Practice of Health Service Provider* - Health Records Act 2001**

Where a health service provider transfers or closes its business, it must publish a notice in a newspaper circulating in the local area stating that the business is to be closed or transferred and giving the individual the opportunity to elect to retain health information or transfer health information to a health service provider nominated by the individual.

***Making Information Available to Another Health Service Provider* - Health Records Act 2001**

If an individual requests a health service provider to provide health information to another health service provider then that information must be provided.

In medical practice this principle is almost always adhered to but now has legislative weight.

What is Health Information?

Health Records Act 2001 (Vic)

The *Health Records Act* applies to all "health information" held in the public or private sectors. This would mean that it applies to health information held by solicitors on behalf of clients.

Under Section 2, health information is defined broadly to include information or an opinion about physical, mental or psychological health, information about the health services provided or to be provided, personal information collected to provide a health service, genetic information, and information in connection with the donation of body parts.

An organisation holds health information if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the documents are situated, whether in or outside Victoria.

This would suggest that, for example, the general practitioner who holds a report from a specialist has that report in his or her possession and therefore, under the access provisions, would have to provide it.

It is not clear how this would sit with the High Court decision in *Breen v Williams*[1] that grants the individual doctor ownership of what they write.

The *Privacy Amendment (Private Sector) Act 2000* also applies to all health services regardless of size. The guidelines to the legislation indicate that health information is considered especially private and personal. However the guidelines also recognise that it is essential for health service providers to share information about individuals.

Implications For Practice

Clients are now entitled to access medical records from 21 December 2001. It is unclear how the retrospectivity provisions of the *Privacy Amendment (Private Sector) Act 2000* will apply or be interpreted. Access may apply retrospectively if the information is used or disclosed after 21 December 2001, unless it causes an unreasonable administrative burden or will cause the organisation unreasonable expense. Access may also be granted retrospectively if the health information is part of a "continuous record". It is not clear whether a general practitioner's records spanning many years would be a continuous record or a series of separate records. My experience in practice is that some private doctors and hospitals, most notably those run by Mayne Health, are granting access to private medical records regardless of whether they are pre or post 21 December 2001. Other private hospitals and doctors are refusing to provide medical records prior to 21 December 2001.

As of 1 July 2002, Victorian clients will not have to rely on the *Privacy Amendment (Private Sector) Act 2000* any longer, as the *Health Records Act* 2001 provides for access to records. Section 25 provides an individual access to the following health information collected before 1 July 2002:

- a history of the health, illness or disability of the individual;
- any findings on an examination of the individual in relation to the health, illness or disability of the individual;
- the results of an investigation into the health, illness or disability of the individual;
- diagnosis or preliminary diagnosis;
- a plan of management or proposed plan of management of an illness or disability;
- action taken or services provided by or under the directions of a health service provider in relation to the individual;
- personal information about the individual in connection with the donation or intended donation by the individual of body parts; and
- genetic information about an individual which is or could be predictive of the health, at any time, of the individual or any of his or her descendants.

For practical purposes this is essentially the entire medical record. Section 29 provides that access does not have to be an actual copy of the record, or a right to inspect the record (but can be if the doctor agrees) but must at least be an accurate summary of the health information.

In summary, clients can access all medical records after 21 December 2001. For medical records prior to that time they can currently access them in limited circumstances. As of 1 July 2002, clients can access all their medical records, but medical records before 1 July 2002 may only be provided in summary form. This may not change the existing situation greatly but will reduce costs. Hopefully the practical reality of the change in legislation will be that doctors do provide the actual medical record, rather than a summary, given the restriction on the fee that they can charge. However, given doctors' historic reluctance to hand over their medical records, they may well opt to only provide a summary for those records pre 21 December 2001.

Access to private medical records is likely to make it easier for plaintiff lawyers to advise clients about the merits of a claim early in the claims process. It is also likely to significantly reduce the time taken to investigate personal injury cases as it will avoid the considerable delays that occur when doctors decide whether or not to provide a medical report and seek legal advice about the provision of the report. ▶

Access by Defendants to Medical Records

The Transport Accident Commission and the Victorian WorkCover Authority require consent by claimants for release of medical records to them in order to process claims.

Arguments exist about what the scope of such consent is. The consent purports to be an enduring consent but the fact that consent must be given otherwise the claim is invalidated also raises the issue of whether the consent was given under duress. The obligation on health service providers to ensure that information is only used and disclosed in accordance with the privacy legislation means that many doctors will be confused about what they can and cannot provide.

"An organisation must not collect sensitive information about an individual unless the individual has consented..."

All the protection afforded by the legislation is effectively nullified by the consent of the individual to disclosure of that information. It is not for the doctor to determine issues of duress.

The consent provided under the statutory schemes only applies to that medical information relevant to the case. It may be necessary to educate the medical community about their obligations under the privacy legislation and the penalties they potentially could face for breaches of privacy by providing information that goes beyond the scope of the consent.

Doctors should also be advised that the most recent consent form they receive is the one that they should be relying on. Plaintiff lawyers need to carefully consider the wording of their letters to doctors and consent forms signed by clients to ensure that they are appropriate and do not jeopardise a client's ongoing TAC or WorkCover claim.

The Victorian WorkCover Authority and the Transport Accident Commission have been known in the past to provide information to each other about an individual claimant's case. On analysis of both the federal and Victorian legislation this is clearly a breach of the claimant's privacy, unless consent has been obtained. Attempts by statutory authorities to obtain information outside the scope of the consent, or to disclose private information outside the scope of the consent, would be a clear breach of the legislation.

Doctors have also asked whether this legislation means that they have to get written consent to provide patient information to a specialist to whom they are referring the patient. Some doctors are already getting patients to sign consent forms for such referrals. On analysis of the legislation such consent forms are unnecessary. The fact that the patient sees the specialist is sufficient consent to the provision of the information. Further, the sharing of information amongst health professionals is likely to be a "primary purpose", or a directly related secondary purpose, and therefore authorised by the legislation. Obviously doctors would not be able to transfer patient information to other doctors without the patient's knowledge, however even in absence of this legislation I would consider that to be a breach of confidentiality.

The fact that plaintiffs can now access their medical records could also be used by defendants to seek discovery of such medical records. If the plaintiff chooses not to access the records the defendant may be able to compel the plaintiff to do so. Access to any medical records by the defendant would, of course, be subject to arguments about privilege. It may be that in reality the situation is not significantly different from a defendant's current ability to subpoena the plaintiff's past medical records and argue the question of privilege before the court.

Private Information Other Than Health Records

The federal privacy legislation also applies to lawyers in our practices. This means that we must all look at our obligations under the legislation and ensure that we comply.

Clients have a legislative entitlement to access their files. On the face of the legislation it appears that clients can access all the information collected about them. To date, this provision has not been tested by the courts but on the face of the legislation there is no exception for what might be called a solicitor's "working notes".

There are some practical steps that lawyers should take:

- Modify fee and retainer agreements, or initial advice letters, to advise clients of your privacy plan and advise them that they can obtain a copy of that plan.
- Advise clients that they have an entitlement to access their file.
- Ensure that everything that is on the file is accurate. If there is a dispute about the accuracy of information, record the fact that there is a dispute.
- Ensure that staff know about the privacy legislation and their obligations under it. This might be something as simple as reminding people not to discuss cases in lifts.
- Make sure that information is collected in accordance with the legislation.
- Advise the client to whom their information may be revealed.
- Obtain consent for using the information other than for primary purposes.
- Ensure client information is stored securely. PL

Footnote:

[1] [1996] 186 CLR 71.