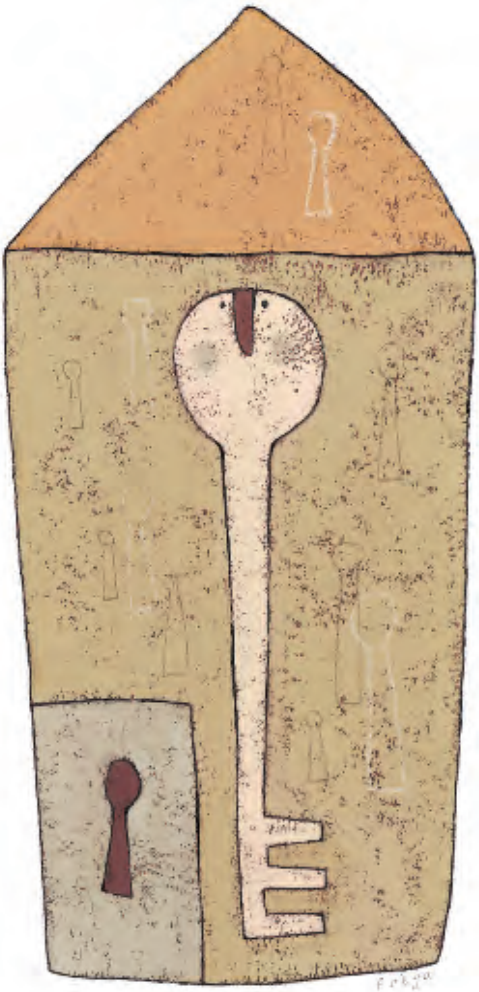
Private Lives

YOUR GUIDE TO PRIVACY LAW IN VICTORIA



Produced by the Victoria Law Foundation

Preface

This booklet is not a manual for privacy officers or managers who are responsible for managing their organisation's privacy policy although they may find it a useful tool in helping consumers and other members of the public who have queries about privacy. The booklet is intended for general readers or consumers who want to know how privacy laws protect their privacy and how they can exercise their rights under these laws. For this reason, the booklet gives emphasis to those aspects of the privacy laws that are likely to be of most interest to the general public – finding out what personal information may be collected lawfully by organisations; how this information is protected from misuse and improper disclosure; and what redress you may have if your privacy is breached.

You may choose to read the whole text from start to end or you may use the detailed table of contents to find issues of particular interest. The booklet is cross-referenced to help the reader make connections across the topics.

The booklet is also available electronically on the internet: www.victorialaw.org.au

This booklet is a general guide to the privacy laws that affect Victorians. It is not intended as a substitute for legal advice. In case of a dispute, you are strongly urged to seek the assistance of a lawyer or one of the expert agencies listed in the back of this booklet. The law in this booklet is as at May 2008. While care has been taken to ensure the accuracy of the material contained in this publication, no responsibility can be taken for any errors or omissions.

Acknowledgements

A number of people have contributed to this booklet, particularly staff of the Office of the Victorian Privacy Commissioner, the Office of the Victorian Health Services Commissioner and the Department of Human Services, including Fahna Ammett, Brent Carey, Michael McDonald, Anne Mullins, Dianne Scott and David Taylor. The Victorian Privacy Commissioner, Helen Versey, and the Health Services Commissioner, Beth Wilson, have been generous in their support and funding of this publication. Meredith Carter of the Health Issues Centre and Peter Devine from the Association of Independent Schools also made many useful suggestions. Our thanks also go to the varied cross-section of readers in the Ballarat area who tested the draft and provided valuable feedback from a consumer perspective.

Contents

Introduction

Privacy is the right to be left alone. It includes stopping or setting limits on intrusions into your:

- body (with invasive medical practices or procedures);
- place of residence;
- personal mail, telephone calls or other private communications; and
- personal information.

This booklet is about the last of these – information privacy – and the laws that protect it.

The fundamental right to information privacy is enshrined in international law, at the Commonwealth level and in Victorian privacy laws. This is part of a worldwide trend. Most European countries, New Zealand, Hong Kong and Taiwan have privacy laws for the public and private sectors.

The explosion of information technologies such as the internet, e-mails, smart cards, electronic scanning and computerised data matching gives us more ways to receive and manage a vast array of information more speedily and effectively. Information that once took years to acquire – if it was available at all – is now easier to get and to handle. In an open society we value this free flow of information.

However, the information revolution has its dangers. It is easier than ever before to gather information about individuals, to store, share or use it for a range of purposes.

We expect our personal information will remain private and secure. Now that information processing is more common, more people can intrude upon our privacy and misuse personal information.

Benefits of having privacy laws

Privacy laws give consumers legal protection and enforceable rights. These laws give you more say in how your personal information is collected and used and who gets to see it. With exceptions that are covered later in this guide, generally these laws are designed to:

- make sure organisations that collect and use personal information about you do so responsibly and wherever possible with your knowledge and consent;
- give you the right to know what information about yourself, including sensitive health information, is collected and used;
- give you the right to request an organisation that holds personal information about you to correct it if it is wrong; and
- enable you to set right any interference with your information privacy by making complaints and having them resolved.

Three information privacy laws apply to Victorians

Victorians have rights and responsibilities under three privacy laws:

- the Victorian *Information Privacy Act* 2000 (referred to in this booklet as the *Information Privacy Act*);
- the Victorian *Health Records Act* 2001 (referred to as the *Health Records Act*); and
- the Commonwealth *Privacy Act* 1988 (amended by the Commonwealth *Privacy Amendment (Private Sector) Act* 2000) (referred to as the Commonwealth *Privacy Act*).

Laws protecting your privacy

Victorian *Information Privacy Act*
Covers personal information (but not health information) held by public sector organisations including local councils

Victorian *Health Records Act*
Covers personal health information held by public and private sector organisations including local councils, employers and schools

Commonwealth *Privacy Act*
Covers personal information and health information held by Commonwealth public sector organisations and many private sector organisations

Other laws protecting privacy
eg *Surveillance Devices Act* (Vic)
Telecommunications (Interception and Access) Act (Commonwealth)

The three Acts are similar, but there are also some important differences, which are explained in this booklet. (For example, see pages 18–19 for how your rights to access health information vary according to when the Acts became enforceable.)

The *Information Privacy Act* became fully enforceable from 1 September 2002. Administered by the Victorian Privacy Commissioner, this Act covers most personal information (but not health information) held by Victorian public sector organisations.

The *Health Records Act*, a companion to the *Information Privacy Act*, became fully enforceable from 1 July 2002. Administered by the Health Services Commissioner, this Act applies to health information held by the Victorian public sector and by private sector organisations across Victoria.

The Commonwealth *Privacy Act*, administered by the Federal Privacy Commissioner, covers most forms of personal information, including health information, held by the Commonwealth public sector and much of the private sector across Australia.

Health privacy is therefore covered in the Commonwealth *Privacy Act* and the Victorian *Health Records Act*. Under both Acts you have a right of access to your own health records. Health service providers and those who hold health information are required to manage your personal information in ways that protect your privacy.

Why a separate law for health information?

The Victorian Parliament separated its two Acts because health information, the most sensitive personal information, needed special treatment. Consumers use health services across both the public and private sectors all the time, and only State laws can regulate the public hospital system and state government agencies. The Victorian government decided that it was necessary to have uniform standards across the public and private sectors.

Privacy and Freedom of Information

The Commonwealth and Victorian *Freedom of Information Acts (FoI Acts)* remain in force alongside the privacy laws. FoI laws exist to help you get access to documents held by government agencies, including your personal information (with some exceptions). By contrast, privacy laws cover the full cycle of collection, use and disclosure, storage and disposal of personal information, and provide other benefits not available under FoI.

The Victorian *FoI Act* regulates access to personal and health information held by public sector agencies such as government departments, local councils and public hospitals. Changes to the *Freedom of Information Act* give you means of access to health information in the public sector that are also available in the private sector under the *Health Records Act*.

Other laws affecting privacy

Privacy is also covered in other legislation. For example, in Victoria, the *Surveillance Devices Act* 1999 controls the use of surveillance devices and restricts the communication and publication of records of private conversations and activities gained through the use of those devices. That Act also restricts the use of tracking devices and computer surveillance devices. The *Equal Opportunity Act* 1995 makes it unlawful to ask people for sensitive personal information, such as marital status, which may be used to discriminate against them.

At the Commonwealth level, the *Telecommunications (Interception and Access) Act* 1979 protects the privacy of your telephone calls and the *Telecommunications Act* 1997 makes strict rules for carriers and service providers in their use of personal information about customers.

The privacy principles in the privacy laws do not override other legislation making rules about personal information. If there is any inconsistency with such a law, the provisions in that other law will override the general standards in the privacy laws. For example, the Victorian *Local Government Act* 1989 requires certain personal information collected by councils to be made available for public inspection.

What information do privacy laws cover?

Personal information is information about an individual whose identity is clear or can reasonably be worked out from that information. Personal information can include opinions and does not have to be true. Typical personal information includes your name, address, age, financial status (such as your eligibility for concessions or benefits) and family information (such as who lives with you). The definitions in the various privacy laws cover documents, photographs, electronic material (such as voice mail and video recordings) and digital databases.

Sensitive information is information (including opinions) about a person's racial or ethnic origin; philosophical or religious beliefs or affiliations; political opinions; membership of a political association, professional or trade association or union; sexual preferences or practices; or criminal record.

Health information is a specific type of personal information. It can take a number of different forms, including records or information about:

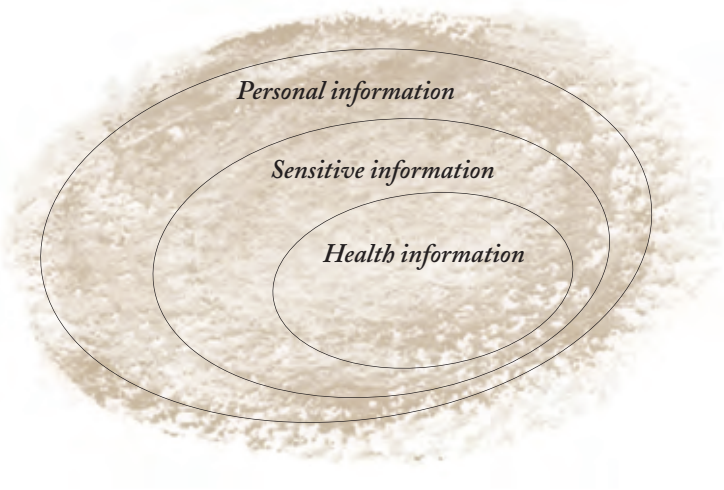
- your physical, mental and psychological health, including any disability;
- treatments you have received;
- donation of body parts; and
- genetic predictions relating to your health or that of your descendants.

Health information could be collected or used in the course of services such as:

- health checkups;
- diagnosis or treatment of illness, injury or disability;
- provision of palliative care, aged care and disability services;
- the dispensing of prescriptions;
- applications for health concessions and benefits;
- applications for life and travel insurance and superannuation; and
- during the course of employment or school attendance.

Under the *Health Records Act* it may be a breach of privacy if your health information is disclosed to someone else by way of an overheard conversation

It is important to remember that privacy laws *do not* apply to information that you collect, use or disclose only for your own personal, family or household affairs.



Source: Office of the Federal Privacy Commissioner

Who has to comply with the privacy laws?

The *Information Privacy Act* applies across Victorian state and local government. It includes departments and agencies such as police; schools and hospitals; local councils; statutory office-holders such as the Auditor-General, and organisations like the Equal Opportunity Commission, the Country Fire Authority and the Environmental Protection Authority. It covers government ministers and parliamentary secretaries but not in their roles as Members of Parliament. The Act extends to private sector organisations only where they provide services to State government agencies under a contract that states the company is covered by the privacy laws. Possible examples are school bus operators or privatised public transport companies.

The *Health Records Act* applies to any public or private sector "organisation" that provides a health service or holds health information relating to individuals in Victoria. An organisation is not limited to health service providers.

In the health field, the law extends to **health service providers** including:

- medical practitioners – GPs and specialists;
- dentists;
- nursing services;
- pathology services;
- pharmacists dispensing drugs;
- private and public hospitals, day procedures and community health centres;
- providers of allied and complementary health services such as physiotherapists, osteopaths and optometrists;
- providers of palliative care services, supported residential services and aged care services such as nursing homes and hostels;
- local councils providing health services such as immunisations and home care;
- providers of mental health services, including psychologists; and
- providers of disability services.

Non-health service providers and Members of Parliament are also required to comply with the privacy laws if they hold health information. Examples of Non-health service providers include insurers, gymnasiums, employers, child care centres, kindergartens and schools. These organisations may also be classed as health service providers to the extent they provide a health service as part of their operations. For example, a school will be classed as a health service provider when it is providing school nurse or counselling services.

The Commonwealth *Privacy Act* applies to Commonwealth government agencies such as Centrelink and to all private sector businesses with an annual turnover of more than $3 000 000. Smaller businesses that:

- provide a health service; or
- trade or sell personal information; or
- are arms of businesses with an annual turnover of more than 3 000 000 must also comply.

Other small businesses may choose to comply with the privacy scheme if they wish, but are not required to do so.

How do the laws protect your privacy?

The privacy laws contain **privacy principles**. These are similar across the three Acts, although the *Health Records Act* has two extra principles unique to health service providers. (See pages 33–35)

Together, the privacy principles set standards that organisations must meet when they collect, store, use or disclose personal information. Privacy is interfered with when an organisation's actions contradict or are inconsistent with any of the privacy principles or any other requirement of the privacy laws.

Under the Commonwealth *Privacy Act* and the *Information Privacy Act* (but not the *Health Records Act*), organisations or industries have the option of registering their own privacy code or complying with an existing approved code of practice instead of the information privacy principles. The relevant Privacy Commissioner must first assess the draft code and agree that the standards proposed are equal to or stronger than those set out in the principles.

Plain language summaries and discussion of the privacy principles can be found on the web-sites of the Offices of the Commissioners (see pages 44–45). For example see www.privacy.vic.gov.au for basic explanations of the Victorian Information Privacy Principles. Some of the main issues for consumers are highlighted in the following pages.

Organisations must have privacy policies

The privacy laws require organisations to have policies on how they manage personal and health information and to make those policies available to the public. If you ask them, organisations must tell you what sort of personal information they hold, for what purpose, and how they collect, store, use and disclose that information.

Collecting personal information

Rules for collecting personal information

Organisations are allowed to collect your personal information only if it is necessary for their functions or activities. They must be able to identify the main purpose for which they are collecting it. This is called the primary purpose. They should tell you why they need your personal information and which law, if any, requires it. If they do not, ask them. They should give a specific reason such as "The teacher must be able to contact you if your child has an accident at school", or "The Council needs it to register your pet". If it is practicable for them to deal with you anonymously, and that's what you prefer, the laws allow it. Primary and secondary purposes are explained further under "Using and disclosing personal information" below.

The privacy laws allow collection of personal information without your consent where collection is authorised by another law, such as that requiring pharmacists to record your Medicare number before they sell you Pharmaceutical Benefits Scheme (PBS)-listed medications, or that relating to councils issuing building permits.

Organisations must collect information fairly, without tricking or bullying you into it. They must also avoid unnecessary intrusion. This means they should normally approach you directly and not ask other people for information about you, unless the law allows it and you are not capable of giving it (for example, you are too ill at the time). If information does need to be collected from someone else, you should be notified as soon as practicable of what information was collected, and why (but see page 20 on limits to right of access).

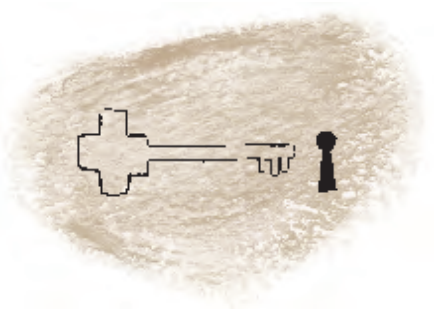
Organisations collecting personal information must be open and not secretive in their processes. They should tell you what personal information they need and why and how they collect it. For example, if your name and address are essential but your telephone number is just a matter of convenience, they should say so. You can then decide what other personal information you wish to provide.

Eleni takes up a new job and the superannuation officer asks her to fill out a form detailing information such as her age, next-of-kin's details, tax file number, employment history and medical history. Eleni is reluctant to fill out the form, but the superannuation officer insists because the super scheme will not be able to establish her entitlements or potential benefits. The super officer is right, but Eleni's employer can only use the information for that purpose. The collection is authorised in this case by the Government Superannuation Act *1999.*

Special protection for sensitive information

Sensitive information is information about your racial or ethnic origin; political opinions; membership of a political, professional or trade association or union; philosophical or religious beliefs or affiliations; sexual preferences or practices; or criminal record. The *Information Privacy Act* and the Commonwealth *Privacy Act* place special limits on the collection of this information.

The Commonwealth *Privacy Act* also recognises health information as sensitive information. The *Information Privacy Act* does not do this, because health information is protected by the companion Victorian law, the *Health Records Act*.



Access to your personal and health information

One of the most important features of the privacy laws is that they give you a legally enforceable right of access to your personal and health information. If you are not physically able to seek access, you can ask your guardian or authorised representative to request it for you.

Making a request for your information

Many organisations nominate a staff member to act as their Privacy Officer, to oversee the organisation's

privacy policy, deal with requests for access and receive complaints. This is the person you should contact when you have a concern or a request for access to your information.

You do not have to give a reason when you ask for access to your personal or health information. However, it might help the organisation to find the information you want more quickly if you tell them exactly what you want to know. Some records can be quite detailed and complex so if there is something specific you want to check – such as a particular test result, for example – you might want to clarify that this is all you seek.

Remember, privacy laws set minimum standards. If an organisation is happy to allow you access to more than the minimum required under the law, then it can, as long as any restrictions on access required by law are followed (see below).

Some records, especially health information, contain highly technical or coded information, which you may not be able to understand without an explanation. In such an instance, you have the right to ask for an inspection of the records and an explanation from a health service provider, rather than asking just for a copy. (A fee may be charged. See page 24.)

The organisation may ask you to put your request in writing (in a letter, fax or e-mail). This is important, especially if your request for information is complex (for example the organisation may hold information about you in different places, or may have to consult staff in different locations).

Establishing your identity

If you are not well known to an organisation it has to ensure you are who you say you are to protect the information from possible misuse. Before sending you personal information, an organisation may want to check your current address, facsimile number or e-mail address and ask you to confirm receipt. If the organisation allows telephone transactions for high-risk services such as banking, it should insist you use your PIN number and password. The organisation should also check your identity before giving personal information to you over the telephone.

Access to information under Victorian law

Personal information and health information from public sector organisations

Some organisations in the Victorian public sector may give you access to your personal information or health information if you approach them informally. However, the enforceable way to seek access to your personal information and health information held by Victorian public sector organisations or local councils is by applying to the organisation under FoI law. Each agency will have an officer who handles all FoI requests in that agency.

Under the Victorian *FoI Act*, you have a right to receive a copy of your health information or to view your file. When the *Health Records Act* came into force, the *FoI Act* was changed to allow two new forms of access: receiving an accurate summary or an explanation of your health information.

Organisations providing services to public sector agencies under contract are not usually subject to FoI legislation, but you should check your access rights through their privacy officer. The Commonwealth *Privacy Act* might cover them or the *Information Privacy Act* might allow access where FoI does not apply.

Health information from private sector organisations

Access to information through FoI applies only to the public sector, so if private organisations hold your health information the process is different.

You can seek access to your health information in the private sector under either the *Health Records Act* or the Commonwealth *Privacy Act*, or both. If your

medical records are held by a Commonwealth agency, you can generally make a direct application to the agency.

The notes made by a private health service provider on a patient's record belong to the provider. Before the privacy laws came into force, providers made their notes knowing that patients or clients did not have a right of access to these notes. Now health providers and others know that their clients can access what they record about them. Health providers were given time to adapt to this change of approach. In Victoria, the *Health Records Act* created two types of rights of access depending on when the information was collected.

1. If you ask for access to health information collected **on or after** 1 July 2002, access can be by way of the full range of legal options:
   - taking notes while inspecting the information; or
   - receiving a copy of the health information, or a print-out of that information if it is in electronic form; or
   - receiving an accurate summary, if you and the organisation agree that a summary is appropriate; or
   - being given an opportunity to see the record and, where the health information is held by a health service provider, an explanation of the information by the health service provider. If the organisation is not a health service provider, it may allow an explanation to be given by a suitable health service provider, but it is not legally obliged to do so under the Act.
2. If you ask for access to health information collected by a private sector organisation **before** 1 July 2002, access may be granted in any of the above ways, but only if the organisation agrees. If they do not agree, you are entitled only to an accurate summary of your information.

Dr Alomes refuses Carmen, a patient, access to her health records because, he says, it contains information collected before July 2002. He does not mention that he is also worried about Carmen's reaction if she sees some critical personal remarks he had written one day when Carmen had become very upset and yelled at him in his surgery. Carmen contacts the Office of the Health Services Commissioner who negotiates an outcome that satisfies both parties. Dr Alomes is made aware that he has breached the Health Records Act, *which entitles Carmen to have access to the pre-July 2002 information, but only in the form of a summary that would exclude his comments about her personality. Carmen gets a summary for the period up to 30 June 2002 and a full copy of all information since that date. Because he has not understood her rights, Dr Alomes also apologises to Carmen.*

Access to personal information under Commonwealth law

Under the Commonwealth *Privacy Act*, distinctions are made between information collected and handled by government agencies (like Centrelink and the Australian Taxation Office) and information collected and handled by the private sector such as insurers and department stores. The private sector was only covered from 21 December 2001. Under the Commonwealth Act you have no right of access to information collected before that starting date unless the organisation holding that information uses it after 21 December 2001. (Compare this arrangement with the Victorian *Health Records Act* page 18.)

If your personal information is held by a Commonwealth government agency, you have right of access even if the information is much older and

not even used. You should apply directly to the agency. All Commonwealth agencies are subject to the Commonwealth *FoI Act* in a similar fashion to the Victorian *FoI Act* (but note the exceptions listed on pages 42–43).

Courtesies

Access should always be provided in a considerate way. For example, it is not acceptable for someone to discuss your personal information in a busy, open public space such as a reception counter and it also may be a breach of privacy if your health information is disclosed to another person in this way. Nor is it reasonable to expect you to inspect large quantities of information while standing at a public counter. Therefore, you should ask the organisation to provide a private area where you can inspect the information or have it explained to you. Organisations are entitled to have a staff member supervise inspections to ensure records are not removed or damaged.

Limits to right of access

There are limits on your right of access to personal information and health information. Access to your health information can be refused in limited circumstances under the privacy laws and the *FoI Act*. The main reasons an organisation may lawfully refuse are where:

- the organisation thinks your having the information would pose a serious threat to your life and health or that of anyone else; or
- refusing access is required by law; or
- granting you access to information would have an unreasonable impact on the privacy of anyone else; or
- the information was provided by someone else in confidence.

If an organisation refuses you access it is required to tell you the reasons in writing. It should also tell you about any process it has for reviewing the decision, and the process you can follow if you wish to object to the decision.

A second opinion on serious threat to life or health

The *Health Records Act* and the *FoI Act* both allow for a second opinion when you apply for health information and the organisation says that granting you access under either Act would constitute a serious threat to your life or health. The Acts allow you to choose an independent health service provider (or accept an independent person nominated by the organisation) to give a second opinion about the decision. If this independent person is satisfied there is no serious threat to your life or health they can allow you to inspect your information or copy it if you wish and discuss it with you. However, the independent person may agree with the decision not to grant you access. If appropriate, this person could explain the reasons for refusal to you. There may be a fee for this service (see below).

Appealing against a refusal

Under the *FoI Act*, there are internal review mechanisms in some cases and the right to appeal to the Victorian Civil and Administrative Tribunal (VCAT). In some circumstances you can also complain to the Ombudsman.

The *Health Records Act* gives an additional option when you have been refused access to your information: in some cases you may seek conciliation by the Health Services Commissioner. If conciliation is successful, the agreement can be enforced. If it is not successful, you can still appeal to VCAT. For more information about conciliation, see "Complaints" below.

If a private sector organisation refuses you access to your personal or health information, you can complain first through the Health Services Commissioner and, if that is not successful, appeal through VCAT.

How to get access to your information

Step 1

Approach the organisation with your request

Approach the organisation that has your personal or health information. They will give you one of the following responses:

Agree **OR** ask you to make a formal request

Step 2

Make a formal request (can be made even if you have been refused informally)

If the organisation is in the *public* sector or is a local council write or fill out an FoI application form. Pay the required fee, if any.

If the organisation is in the *private* sector write to the organisation or fill out their application form. Pay the required fee, if any.

If the organisation is a government contracted service provider, how you apply for your information depends on whether it is subject to FoI requirements.

Step 3

If your request is refused

The organisation must give their reasons in writing. Clarify what options and processes are available for challenging and perhaps changing that decision. Your options may include (depending on the particular circumstances):

- a **SECOND OPINION** (if you were refused access to health information because the organisation thought there was a threat to life or health)
- a **REVIEW** within the organisation, for example at a higher level of authority
- **CONCILIATION** by the Health Services Commissioner
- **FORMAL APPEAL** to VCAT.

Fees for access to information

Some organisations may not charge fees for providing access to information because they see it as part of their service or they value the public relations benefits of providing information free of charge.

The *Health Records Act* and the Commonwealth *Privacy Act* allow, but do not require, organisations to charge for providing access. Under the *Health Records Act* you can be charged a fee prescribed (by *Health Records Regulations* 2002) for that manner of access. No organisation can charge you more than the prescribed maximum, and all are encouraged to charge less.

The Commissioners discourage organisations from charging excessive amounts that might deter people from making requests for access. Organisations are particularly encouraged not to charge for simple services where minimal costs are incurred, like letting you view a computer screen or sending information by e-mail. If you are a pensioner, organisations are strongly encouraged not to charge regardless of what format you seek access in or how much information is involved.

As an indication, the Victorian Regulations say that for copies of A4 size black and white pages a private sector organisation may charge up to 20 cents per page; and up to $20 if the organisation incurs costs in staff time or associated costs; and a further $10 if the documents are not stored at the organisation's usual place of business.

The Regulations also set a maximum fee that may be charged by an independent provider for giving a second opinion about a refusal to provide information on the grounds that it would constitute a serious threat to life or health. The Regulations also set a maximum fee for a request that your health information be made available to another health service provider (see pages 34–35).

When an organisation voluntarily gives information to a third party, as permitted under the *Health Records Act* or another law, no fees are charged because this is "disclosure" of health information, not "access".

Under the *Information Privacy Act*, you seek access by way of FoI in the first instance (see pages 17 & 20). You have to pay fees for FoI requests, although some government agencies give concessions to people in financial hardship. There is an application fee of $20 and a search fee of $20 an hour or part thereof. Photocopying is 20 cents for each A4 page and there may be other charges for any additional costs to the organisation.

Service providers contracted to supply services to government are able to charge a fee, consistent with the fee prescribed under the *FoI Act*, for granting access to personal information held by them as agents of government. Ask what the current fee arrangements are.

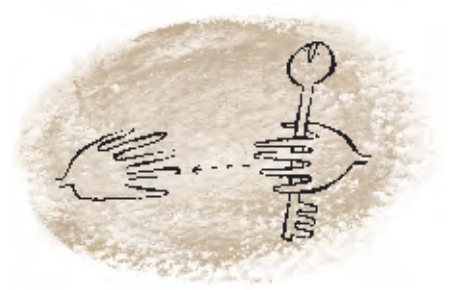
Correcting personal information

Organisations holding your personal information must take steps to see that it is accurate, complete, up-to-date and relevant to the function for which it was gathered. If you find what you believe are errors or omissions in your file and can show the organisation what is incorrect, you can ask that it be put right. Discuss the matter with the organisation because you may be able to agree on ways of correcting the information that satisfy both you and them.

Health service providers can not alter any information that they relied on at the time they provided treatment. However, they are required to add any updating information you provide, if you can establish that it is needed.

If the organisation is not willing to correct your information as you request, you can provide them with a statement about the requested correction. The organisation must attach this statement to your file so whenever the information is handled in the future the user would know about your concerns.

If an organisation refuses to correct personal information it must give you its reasons in writing. At the same time, you could ask whether it has a process for reviewing its decision and what process you can follow if you wish to make a complaint about that decision.



Using and disclosing personal information

Primary and secondary purposes

Usually, an organisation can only use your personal information within its organisation or give it to someone outside the organisation if the use or disclosure is for:

- the primary purpose for which it was collected; or
- a related purpose or, in the case of sensitive information or health information, a directly related secondary purpose, for which you would reasonably expect it to be used or disclosed.

Example 1: *Taut and Terrific is a small fitness centre that sells beauty aids and health foods at its shop. When the supplier goes into receivership, Taut and Terrific strikes a deal with another supplier. The new supplier wants to expand its direct marketing scheme so asks the fitness centre for its client list for its mail order business. Taut and Terrific, anxious to make good its lost income, supplies its client list on a commission basis.*

Before disclosing their clients' personal information for a purpose other than that for which it was provided (to keep track of clients, send them information about their services and bill them), Taut and Terrific should have sought their consent. It is likely that their clients would not expect their personal information to be used for this other purpose.

Example 2: *Three government schools supplied their students' names and addresses to a restaurant and bar that gave the schools a dollar each time a student's family ate there. The schools appeared to be in breach not only of privacy principles but also of the Education Department's guidelines on not promoting alcohol. The practice has now stopped.* (The Age *25 June 2002*)

The Commonwealth *Privacy Act* places additional safeguards on the way the credit industry handles sensitive information about your credit status. Strict penalties apply if these safeguards are knowingly breached.

Other permitted purposes

Organisations can use or disclose your personal information for another purpose if you freely give your consent. However, the *Health Records Act* recognises that there are situations in which it is not practicable to obtain consent. An obvious example: if you become unconscious while being driven to

hospital, the ambulance officers must tell the hospital staff what you told them about how you became ill and other personal information such as your name, age and address.

There are several exceptions to the rule about the use and disclosure of personal and health information (see also the table on pages 42–43). These exceptions include situations where:

- your personal information is to be used for research provided that the research is not published in a way that identifies you and it is not practical to gain your consent;
- if your personal information is disclosed to someone else for research, it is reasonable to believe that the person receiving it will not disclose your identity to anyone else. However, note that the requirements for health information are stricter and there are also statutory guidelines on research that must be observed;
- your personal information is on a public register kept by a body such as your local council. (Public registers often contain personal information not covered by privacy laws but required by other laws to be made available to members of the public upon request. An example is personal information on the planning register.);
- there is a serious threat to your life, health, safety or welfare or that of another person, or to public health, safety or welfare;
- there is a well-founded suspicion that an unlawful activity has been engaged in;
- disclosure would help police or national security agencies do their duty; and
- the law requires or authorises someone to disclose your personal information.

The term "required by law" has a stronger force than "authorised by law". "Required" means an organisation *must* disclose, while "authorised" indicates it *may* exercise its discretion.

George, 68, dies in a car accident when his car runs off a straight stretch of road and hits a tree. George's daughter, Helen, is executor of his will. The coroner requests George's medical records, because he is investigating the cause of George's death and, given George's age, thinks a heart attack may have caused him to run off the road. George's GP advises Helen that, although she is George's legal representative and so would usually have to give her consent to a disclosure of George's health information, he is required to hand over the documents to the coroner because the law (the Coroners Act*) requires him to do so.*

Disclosing personal information to police

The privacy laws allow an organisation to disclose your personal information to police or other law enforcement agencies if it "reasonably believes" the disclosure is "reasonably necessary" for reasons related to:

- criminal offences or suspected offences;
- the confiscation of the proceeds of crime;
- the protection of public revenue;
- seriously improper conduct; or
- proceedings of courts or tribunals such as court orders.

The emphasis is on unlawful activity. Suspicions of unlawful activity must be based on reasonable grounds – rumour or gossip is not enough.

The word "reasonable" implies an approach based on good reasons balancing all relevant factors in a situation. A reasonable belief is what an ordinary person, not necessarily an expert, would think is reasonable in the circumstances.

An organisation is not compelled to disclose personal information to the police, but if it does it

must make a written note stating what was disclosed and the reasons for doing so and file this note.

Registered health service providers, such as doctors and psychologists, can only disclose health information about their patients to the police where the disclosure would not be considered at law to be a breach of confidence. The law allows such confidences to be breached only where it is in the public interest to do so.

Other privacy principles

A number of privacy principles have been discussed so far, including collecting, accessing, correcting, using and disclosing information. The following section briefly looks at some other principles.

Responsible storage and disposal of personal and health information

Organisations must protect personal and health information against misuse or loss and against unauthorised access, modification or disclosure. For example, you should expect hard copy records of your information to be locked away and computerised records to have password protection. Your personal information should be available only to those people who need it to carry out their duties.

Organisations are required to destroy or permanently de-identify personal information when it is no longer needed. However, public sector agencies can only destroy information in accordance with the privacy laws or some other more specific law such as the *Public Records Act* 1973 (in Victoria).

The *Health Records Act* obliges health service providers to keep their records for at least seven years after the last service (for an adult) or until the patient is 25 (for a child). A non-health service provider must destroy or permanently de-identify health information once it is no longer needed.

In disposing of information, organisations must take care. They cannot simply dump the files in the garbage. (That has led to breaches of privacy in the past.) Responsible organisations shred or pulp paper files and use specialised techniques to ensure that personal information in electronic format cannot be retrieved after being deleted.

Permanently de-identifying information means removing from the record forever any information by which you may be identified. Removing your name and address is a good start, but may not go far enough. An organisation should not be able to re-establish your identity.

Restricted use of unique identifiers

Unique identifiers are markers such as your tax file number (TFN), Medicare number, driver's licence number, or other identity number assigned by a public sector organisation to you and no one else. Unique identifiers assigned by governments can only be used by private sector organisations as their own identifier for you if you consent or where it is permitted or required by law. This is to prevent the unlawful matching of data across organisations.

For example, a private sector organisation should generally only use or disclose your Medicare number to provide medical care (including subsidised medicines) financed under Medicare and to fulfil its reporting obligations to the Department of Health and Ageing.

Freda understands that her Tax File Number (TFN) is private and must be kept secure. She is surprised when she goes to open an account and her bank asks for it. When she refuses, the teller says that the Taxation Office would oblige the bank to withhold interest payments from her account unless she provides her TFN.

In this case, the Taxation Office is allowed to match your stated income with bank interest to make it harder to avoid tax – one of the few examples where a unique identifier issued by government is allowed to be used for large-scale data matching. The law lets you refuse to supply your TFN, but imposes taxation penalties if you do not supply it.

Restricted transfer of information overseas and interstate

The Commonwealth *Privacy Act* limits the flow of information outside Australia, and the *Information Privacy Act* and *Health Records Act* limit the flow of information outside Victoria. Organisations are only allowed to transfer personal and health information beyond the relevant border if they reasonably believe the organisation they are sending it to is bound by similar restrictions on the use of that information, or if you consent to the transfer.

Personal information may be transferred with your consent or if the transfer is necessary for the performance of a contract. If your consent cannot be obtained for practical reasons, the organisation can only transfer the information if it is for your benefit and if they think you would be likely to give your consent.

Mario joins a mail order book club but becomes annoyed at their hard-sell telephone techniques. He writes asking to be deleted from their membership list. The monthly catalogues and phone calls persist. A company spokesperson tells Mario his name can not be deleted until next year because the computer program can only be changed once a year. No, the spokesperson says, it is not possible to speed this up because the records are managed by the parent company in the USA. This is news to Mario as he had only ever dealt with a company in Australia.

This case raises issues about personal information being up-to-date and the flow of data outside Australia. When consumers sign a contract they should read the fine print very carefully in case they give their consent to the use of personal information without realising it.

Additional health principles in the *Health Records Act*

The *Health Records Act* has two further principles that are specific to health service providers.

When a health service provider's practice or business is transferred, amalgamated, closed or sold

When one of those events occurs, and a health service provider is not going to provide services in that practice, the provider has several choices. It may keep your health information, or transfer it:

- to the health service provider who has taken over the practice or business (in the case of it being sold); or
- to the patient or client; or
- to a new practitioner nominated by the patient or client.

However, the *Health Records Act* requires the health service provider (or their legal representative) to do three things:

(a) publish a notice in a local newspaper stating what the provider intends to do with the health information (where a significant proportion of clients of the practice or business ordinarily use a language other than English, the service provider must publish that information in appropriate non-English language newspapers);

(b) where practicable, give information in writing to each client regarded by the health service provider as currently receiving a course of treatment; and

(c) display a notice at the practice about what is happening to the practice and the health information.

If the provider decides to keep your health records, and you ask for them, the provider may still keep them but must treat your request as an application for access.

If a practice conducted by a public body closes, the original records that must be kept under the Victorian *Public Records Act* 1973 cannot be provided to the individual, but a FoI request for copies can be made.

The Health Services Commissioner has published statutory guidelines providing further information about this Principle and additional requirements.

Making your health information available to another service provider

The *Health Records Act* allows you to ask a health service provider to make available some or all of your health information to another provider (regardless of whether your first provider collected the information before or after July 2002). You can also authorise your new health service provider to make the request on your behalf. This is different from asking a health service provider to give you your information. It is really switching information from one provider to a new one.

This requirement applies to health service providers in both the public and private sectors, including private practitioners, private health and aged care providers, disability providers and public hospitals.

Milena is moving from Melbourne to live in Gippsland. She has been going to her local doctor and dentist for 10 years and, because of her history of asthma and recent major dental work, wants to make sure her new doctor and dentist have all the information about her health history. Once she is settled in the country and has found a new doctor and dentist, Milena can ask her Melbourne doctor and dentist to provide copies of her records to her new ones, or ask her new providers to make the request on her behalf.

Complaints

You can only complain about the mishandling of your own personal information, not about anyone else's. However, you may be able to act for someone who is not capable of acting independently, such as a child or a person who has a disability or is too ill.

The procedures set up under all three privacy Acts emphasise a stepped approach to resolving complaints, with legal enforcement as a last resort.

Step 1: Deal with the organisation first

As a first step, you should try to resolve your concerns with the organisation.

Ask who is the best person in the organisation to handle your concern. Most big companies, local councils and government agencies have a privacy officer who is trained to help resolve complaints about personal information. The organisation's privacy policy may give a contact point and tell you the steps you should follow.

It is good practice to put your concerns in writing, including:

- the facts that caused your concern (what happened, when and where);
- the consequences for you (what was or will be the effect on you); and
- a satisfactory resolution (what you would like to happen now to resolve your concern).

The appropriate Commissioner will ask whether you have tried to sort out the problem with the organisation before you lodged a formal complaint with the Commissioner. If you have not done this, they may refer the complaint back to the organisation. The Commissioner may be able to help you approach the organisation about the problem.

Each Commissioner has produced a complaint form you can use if you prefer. The forms can be printed from the relevant website or obtained from their offices (see pages 44–45 for contact details). The Commissioners also provide a variety of printed information about how to make a complaint.

Step 2: Conciliation through the office of a Commissioner

If you haven't been able to resolve your complaint with the organisation, you may want a Commissioner to deal with it.

The three Commissioners all emphasise conciliation in trying to resolve complaints.

Conciliation gives the parties the chance to talk to each other and consider each other's point of view. This can lead to a mutually satisfactory solution, which can also be creative and tailored to the situation. Conciliation is much cheaper and faster than formal legal proceedings.

You will need to give all the details in writing, in the same way as in Step 1. The Commissioner's staff may ask you to fill out a complaint form. Commissioners may refuse to accept a complaint if they decide it is not a serious complaint, it is about something very unimportant, or if it happened too long ago.

When you became aware that your privacy may have been breached you should try to make a formal complaint to the:

- Victorian Privacy Commissioner within forty-five days of that date;
- Health Services Commissioner within twelve months;
- Federal Privacy Commissioner within twelve months.

Under the *Health Records Act* a person cannot be victimised because of making a complaint. It is an offence to threaten, intimidate or try to persuade someone not to complain.

Which Commissioner?

You can lodge a complaint under any of the three privacy laws. When deciding where to lodge a complaint, you should consider which Act seems to cover your problem.

- The *Information Privacy Act* covers personal information (but not health) in the Victorian public sector, including local councils and those private organisations contracted to provide government services.
- The *Health Records Act* covers only health information and other personal information collected to provide, or in providing, a health service in both the public and private sectors in Victoria.
- The Commonwealth *Privacy Act* covers health and non-health personal information in the

Commonwealth public sector and much of the private sector across Australia. The Federal Privacy Commissioner is also responsible for complaints about credit reporting, tax file numbers or spent (old) convictions relating to Commonwealth offences (see page 40). Victoria has no spent convictions law, but if you are concerned about the privacy of criminal record information contact the Victorian Privacy Commissioner's Office.

First, confirm that the Commissioner you contact has the power to deal with your complaint. If you apply to the wrong Commissioner, they will refer you to the right one. Remember, there are time limits on lodging complaints (see above page 37).

Where a complaint could be dealt with under either State or Commonwealth law (in health matters, for example), you can choose the one you feel would be best for your situation. The Office of the Federal Privacy Commissioner is in Sydney, and conciliation is usually done by mail or telephone. If you want to try to resolve the problem face-to-face, it may be better to complain through the Victorian Health Services Commissioner's Office in Melbourne.

Step 3: Making a decision when conciliation is not possible

When conciliation is not possible or fails, a decision will be made by an independent authority as shown in the table opposite. While the complaints processes are similar, there are some differences in the way they work, especially at this later stage.

The three steps of the complaints processes are summarised in the following table.

Complaints under the *Information Privacy Act*

Victorian government agencies and local councils had a year to get ready for the formal complaints that could be lodged against them after 1 September 2002.

If your complaint is about the **collection** of personal information, it can only be about

Summary of Complaints Procedures

	Complaint to the Victorian Privacy Commissioner	Complaint to the Victorian Health Services Commissioner	Complaint to the Federal Privacy Commissioner (see also "Complaints under a code of conduct")
Step 1	The complaint is referred first to the organisation for a response and, if this does not provide a satisfactory resolution, move to Step 2.		
Step 2	The Commissioner can conciliate it. If conciliation fails, or if the Commissioner thinks another course of action is needed, move to Step 3.	The Commissioner can conciliate or investigate it and make a ruling. The Commissioner can also investigate it if conciliation fails. If you want to challenge the ruling move to Step 3.	The Commissioner can investigate and make a ruling. If this is not complied with, move to Step 3.
Step 3	The Victorian Civil and Administrative Tribunal (VCAT) can hear a complaint and make a binding determination to resolve it.	VCAT can hear a complaint and make a binding determination.	The Federal Court can make binding orders to resolve a complaint.

information collected from 1 September 2001 onwards. But if your complaint is about the use or disclosure or other aspects of your personal information, it does not matter when that information was collected, so long as the breach happened after 1 September 2002.

Complaints under the *Health Records Act*

Complaints are restricted to actions after 1 July 2002, when the Health Privacy Principles became legally binding.

Complaints under the Commonwealth *Privacy Act*

Under the Commonwealth *Privacy Act*, complaints can only be made against:

- Commonwealth and ACT departments or agencies;
- credit providers such as banks or building societies and credit reporting agencies;
- organisations that handle your TFN;
- organisations that ask for or use information about an old criminal conviction under the Commonwealth Spent Convictions Scheme; and
- private sector organisations covered by the National Privacy Principles or by a code approved by the Federal Privacy Commissioner.

Complaints under a code of practice

Some organisations operate under a specific, approved code of practice instead of the formal statutory procedures. A person called a "code adjudicator" can deal with complaints lodged under the Commonwealth *Privacy Act* against organisations covered by an approved code of conduct. A code adjudicator has the power to investigate, conciliate or settle a complaint made under that code. An adjudicator would only act if either:

- you had complained to the organisation and the matter has not been resolved to your satisfaction; or
- the organisation has not responded to you within sixty days from the date that you lodged the complaint.

Under those circumstances, you can either ask the adjudicator to handle the matter or ask the Commissioner to investigate it. Code adjudicators must also decide whether the Commissioner or another code adjudicator is better able to handle the complaint.

Enforcing privacy laws

Commissioners attempt to persuade organisations of the benefits of privacy legislation, and to encourage them to comply with guidelines and advice. They all emphasise conciliation in resolving complaints. However, all three Commissioners have strong powers to enforce the law. The strength of a Commissioner's reaction is likely to depend on considerations such as:

- the seriousness of a breach;
- the severity of the harm done; and
- the extent of the organisation's failure to act to prevent the risk of the breach.

These other powers are explained on each Commissioner's website and in publications issued by them (See pages 44–45).

Exemptions and permissions

All three laws exempt some groups from their operation. All three laws give permission to collect, use or disclose personal information without a person's consent, in certain defined circumstances. The following table shows the main exemptions and permissions.

Main Exemptions and Permitted Uses and Disclosures under the Privacy Acts

Organisations	Information Privacy Act	Health Records Act	Commonwealth Privacy Act
Law enforcement and national security agencies	Limited exemption	Limited exemption	Limited exemption
Political parties and officers in course of proper functions	Not applicable	Not exempt	Exempt
Courts and tribunals (in their judicial capacity)	Exempt	Exempt	Exempt
Media in the course of their duties	Not applicable	Exempt	Exempt
Types of information			
Employee records held by current or former employers	Not exempt	Not exempt	Exempt in private sector only
Access to health information given in confidence to a health service provider about you by another person	Not applicable	Request for access *must* be refused	Request for access *may generally* be refused
Access to personal information that would pose a serious threat to your life or health, or that of another person	Request for access *may* be refused	Request for access *must* be refused	Request for access *may* be refused
Access to certain information in your health record that would have an unreasonable impact on the privacy of anyone else	Not Applicable	Request for access *may* be refused	Request for access *may* be refused
When another law requires disclosure	The provisions in the other legislation prevail to the extent of any inconsistencies with privacy laws		
Personal information contained in a publication generally available to members of the public	Exempt but organisations should follow privacy principles as far as possible	The Act does not cover this issue	Commonwealth's position under review at time of writing
Information held on public registers	Follow privacy principles as far as possible	Act does not include pubic registers	Commonwealth's position on public registers under review at time of writing
Types of activities			
When the organisation believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to a person's life, health or safety, or public safety	Permitted to use or disclose without consent	Permitted to use or disclose without consent	Permitted to use or disclose without consent
When it is reasonable to suspect that unlawful activity is involved	Permitted	Permitted but not if it would be a breach of confidence by a registered health service provider	Permitted
The use of personal information for research and other statistical purposes	Permitted if in the public interest and not for publication in an identifying form, and impracticable to get person's consent	If health information, permitted if in the public interest, and getting consent is not practicable. An Ethics Committee must approve the project in accordance with Commissioner's guidelines.	If health information, permitted if in the public interest, and getting consent is not practicable. An Ethics Committee must approve the project in accordance with Commissioner's guidelines. If non-health information, then only permitted if such use is related to the primary purpose it was collected for, and the person would reasonably expect such a use.

Where to go for help

One of the quickest ways of getting up to date information is through the internet or world wide web (www). Some of the most relevant website addresses are listed below. All of these sites link to other related sites. If you do not have access to the Internet, your local library can probably help you.

Specific information on privacy laws and complaints

Office of the Victorian Privacy Commissioner
Level 11, 10-16 Queen Street, GPO Box 5057 Melbourne, Victoria 3000
Telephone: 1300 666 444 (toll free from anywhere in the State)
Fax: 1300 666 445
E-mail: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Office of the Victorian Health Services Commissioner
30th Floor, 570 Bourke Street Melbourne, Victoria 3000
Telephone: 8601 5200 or 1800 136 066 (toll free for rural and regional callers) Fax: 8601 5219
E-mail: hsc@dhs.vic.gov.au
Website: www.health.vic.gov.au/hsc/

Office of the Federal Privacy Commissioner
GPO Box 5218, Sydney, NSW 1042
Privacy Hotline: 1300 363 992 (local call charge)
E-mail: privacy@privacy.gov.au
Website: www.privacy.gov.au

Copies of laws

Australian laws and regulations are available for downloading on the internet at: www.austlii.edu.au

Information Victoria – sells hard copies of Victorian Acts of Parliament and Regulations, government reports and an updated Victorian Government Directory.
505 Little Collins Street, Melbourne 3000
Telephone: 1300 366 356 (local call charge)
E-mail: bookshop@dpc.vic.gov.au
Website: www.information.vic.gov.au

Consumer and legal advice

Community Legal Centres – free advice from over 40 centres. Check locality near you through the Federation of Community Legal Centres.
Telephone: 9652 1500
Website: www.communitylaw.org.au

Dispute Settlement Centre of Victoria – free advice on dispute resolution and mediation.
Telephone: 9603 8370 (toll free outside Melbourne 1800 658 528)
Website: www.justice.vic.gov.au/disputes

Financial and Consumer Rights Council – provides advice on managing debts and consumer complaints.
Telephone: 9663 2000 or 1800 134 139 (toll free)
Website: www.fcrc.org.au

Law Institute of Victoria – free consultation with a solicitor.
Telephone: 9607 9550
Website: www.liv.asn.au

Office of the Victorian Ombudsman
Level 9, 459 Collins Street, Melbourne, Victoria 3000
Telephone: 9613 6222 or toll free 1800 806 314 (rural and regional clients) Fax: 9614 0246
Website: www.ombudsman.vic.gov.au/

Victorian Civil and Administrative Tribunal (VCAT) – deals with disputes across a range of areas including disputes about privacy under the Information Privacy Act and the Health Records Act.
Telephone: 9628 9830 (Civil Claims List)
Website: www.vcat.vic.gov.au

Extra information on privacy issues

Privacy Law and Policy Reporter, a monthly journal that reviews and analyses privacy issues in Australasia and the Asia-Pacific region.
Telephone: (02) 9385 2233
Website: www.austlii.edu.au/au/journals/PLPR

Australian Privacy Foundation – the main voluntary organisation focused on protecting the privacy rights of Australians. Does not take up individual complaints but works with consumer groups and professional associations to lobby government on privacy policies. The Foundation invites interested people to participate in its activities.
E-mail: enquiries@privacy.org.au
Website: www.privacy.org.au

Liberty Victoria (Victorian Council of Civil Liberties Inc.) – a voluntary body focused on civil rights and freedoms, particularly those expressed in Australian and international law.
4th Floor, 360 Little Bourke Street Melbourne, Victoria 3000
Telephone: 9670 6422
E-mail: info@libertyvictoria.org.au
Website: www.libertyvictoria.org.au

On health specific issues

The Health Issues Centre – an independent community organisation that researches health issues and analyses them from a consumer perspective. Health privacy issues are regularly discussed in *Health Issues Journal*, issued quarterly.
Level 5, Health Sciences 2, La Trobe University 3086
Telephone: 9479 5827
E-mail: info@healthissuescentre.org.au
Website: www.healthissuescentre.org.au

Victoria Law Foundation

Victoria Law Foundation is an independent, non-profit, community benefit organisation providing legal information through grants, publications, programs and events. The Foundation is established under legislation and funded by the Legal Services Board Public Purpose Fund.
See our website at www.victorialaw.org.au

First published 2003
This edition 2008

ISBN 1 87 6045 27 2
Author: Frank Golding
Editor: Kath Harper
Designer: Leon Kustra, The X Factor
Illustrator: Fréya Boyle