FACT SHEET

PRIVACY IN VICTORIA

The right to have personal and health information protected in Victoria and in the Commonwealth

With people becoming more aware about privacy risks, lawyers need to consider legal obligations and rights established by privacy laws.[i]

PRIVACY LAWS

Victoria

The *Privacy and Data Protection Act 2014* ("PDP Act") protects personal information while the *Health Records Act 2001* ("HR Act") regulates health information.

The PDP Act defines personal information broadly. Essentially, it must be recorded, and be about a person who is still alive. Personal information can include CCTV footage, photographs and database entries.

The PDP Act applies to all Victorian state and local government authorities. It applies to public boards, universities, public schools and bodies such as the Transport Accident Commission, Consumer Affairs Victoria or the Victorian Building Authority.

The Office of the Victorian Information Commissioner ("OVIC") regulates privacy which includes approving certain practices and establishing standards for data security.

Health information is defined broadly by the HR Act. The definition not only includes information or opinions about an individual's physical, mental or psychological health; but can be information about any disability (at any time) of an individual; or expressed wishes about health services being provided now or in the future.

The breadth of the definition means the HR Act applies to any health service provider, whether public or private. It also applies to anyone holding health information whether or not a health service is being provided. For instance, an employer holding medical appointment leave application forms holds health information regulated by the HR Act.

Commonwealth

The *Privacy Act 1988* (Cth) ("Privacy Act") protects personal information, health information, and credit information. It applies to Commonwealth bodies, such as Medicare and Centrelink, as well as to private organisations with a turnover of more than $3 Million in a financial year. For example, a private organisation in Victoria with an annual turnover of $3.2million must comply with the Privacy Act.

Some organisations may need to strictly comply with privacy requirements, such as credit reporting businesses or those handling tax file numbers. The Office of the Australian Information Commissioner ("OAIC") can approve codes of practice under the Privacy Act for credit reporting or marketing.

PRIVACY PRINCIPLES

The PDP Act, HR Act and Privacy Act each establish a set of privacy principles that outline how personal or health information should be handled.[ii] While the privacy principles overlap to a great degree, there are subtle differences which may impact how personal and health information is handled at Victorian or Commonwealth levels.

The privacy principles address the following aspects of handling personal or health information:

Privacy Principle	PDP Act	HR Act	Privacy Act
Collection	IPP1	HPP1	APP3-5
Use and disclosure	IPP2	HPP2	APP6
Quality	IPP3	HPP3	APP10
Security and retention	IPP4	HPP4	APP11
Openness	IPP5	HPP5	APP1
Access and correction	IPP6	HPP6	APP12-13
Identifiers	IPP7	HPP7	APP9
Anonymity	IPP8	HPP8	APP2
Transfer of information	IPP9	HPP9	APP8
Sensitive information	IPP10	-	-
Closing a health service	-	HPP10	-
Making information available to another health service	-	HPP12	-
Direct marketing	-	-	APP7

The common privacy principles are outlined below. For more detail, refer to the links at Further Information.

Collection

Personal or health information must only be collected where it is necessary for the collecting organisation's functions. Information should be given to the person whose information is collected letting them know what the information is going to be used for, how to contact the organisation that collected the information, and how to correct the information in future.

Use and Disclosure

Before using or disclosing personal or health information, care must be taken to ensure that the relevant privacy laws are followed. Using personal information for the purpose for which it was collected or for a related secondary purpose is permitted. A specific exception might exist, such as where the law requires the personal or health information to be used or disclosed in a certain way (such as to a court).[iii]

Security and Retention

Reasonable steps need to be taken to keep personal and health information secure and safe from misuse, loss, unauthorised access or disclosure.

If health information is to be destroyed, a note should be made and retained of that destruction; failing to do so is a privacy breach.

Openness

If an organisation holds personal or health information it must have a privacy policy available to the public showing how it deals with that information. These are often located on websites.

Access and Correction

Members of the public may be able to access and correct their personal and health information under privacy laws. In some instances personal and health information may not need to be provided.[iv] Government bodies may handle this type of request through Freedom of Information legislation.

Identifiers

Unique identifiers, such as membership numbers assigned to individuals by an organisation, cannot be assigned or shared across organisations unless there is a real need for that to occur.

Anonymity

Members of the public should not be required to provide personal or health information where it is not

necessary and, where practicable, people should be able to remain anonymous.

Information Transfer Outside Jurisdiction

If an organisation holding personal or health information wants to transfer that information outside of the relevant jurisdiction, then the recipient must have similar privacy protections available either under its own legislation or by agreement.

COMPLAINTS

If a person believes that their privacy has been interfered with, they can make a complaint to one of the following Commissioners:

- For a breach of the HPPs, the Health Complaints Commissioner ("**HCC**");
- For a breach of the IPPs, the OVIC; or
- For a breach of the APPs, the OAIC.

The Commissioners have broad powers to handle privacy complaints, including conciliation powers. The Commissioners may seek submissions from the parties so as to issue a determination. If the person making the complaint remains dissatisfied, he or she can seek review. A complainant must usually first complain to the organisation about which they are concerned. If this has not occurred, the Commissioners may initially refuse to accept the complaint.

If a complaint has been made to an organisation, but was not dealt with to the complainant's satisfaction, then the Commissioners are likely to accept the complaint.

REVIEWS

Victoria

The complainant can request the OVIC or HCC to refer their complaint to the Victorian Civil and Administrative Tribunal ("VCAT") where the respective Commissioner has:

- refused to deal with a complaint; or
- made a determination that the complainant disagrees with.

Time limit: review must be sought within 28 days from the date of notice of the Commissioner's decision.

Cost: No charge

There is a right of appeal from the VCAT to the Supreme Court on a question of law.

Commonwealth

A complainant can request the OAIC to refer their complaint to the Administrative Appeals Tribunal ("AAT"), where the Commissioner has:

referred or dismissed an application;

- made a declaration, direction or determination;
- decided to register (or not) an APP code;
- approved, refused to approve or revoked guidelines.

Time limit: review must be sought within 28 days from the date of notice of the OAIC decision.

Cost: $920 (as at 1 July 2018)

An application can be made to the Federal Circuit Court under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) where the OAIC decides not to investigate or further investigate a complaint.

There is a right of appeal from the AAT to the Federal Court on a question of law.

DATA BREACH NOTIFICATION

If an organisation that is subject to the Privacy Act believes:

- it has breached the Privacy Act; and
- that breach is likely to result in serious harm to any individual whose information is involved in that breach;

then it must notify the OAIC and potentially the person involved.

There are strong penalty provisions resulting to paying the Commonwealth for non-compliance with this section.

FURTHER INFORMATION

HCC: https://hcc.vic.gov.au/

OVIC: https://www.ovic.vic.gov.au

Guidelines for complainants: https://ovic.vic.gov.au/privacy/for-the-public/complaints/

Guidelines to handling complaints by the VCAT: https://ovic.vic.gov.au/privacy/privacy-complaints-at-vcat/

Short guide to the IPPs: https://ovic.vic.gov.au/resource/short-guide-to-the-information-privacy-principles/

VCAT: https://www.vcat.vic.gov.au/

OAIC: https://www.oaic.gov.au/

APP guidelines: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

AAT: http://www.aat.gov.au/

[i] This factsheet only addresses the privacy laws identified; it does not address telecommunications privacy or other privacy issues.
[ii] PDP Act, ss 19 and 20(1); HR Act, s 21(1); Privacy Act, s 13(1)(a).
[iii] for example: PDP Act, ss IPP2.1(g).
[iv] For example, where providing access to personal information would be likely to prejudice the investigation of possible unlawful activity: IPP6.1(h).