Reforming Victoria's privacy legislation

Consultation questions

VICTORIA State Government | Premier and Cabinet

Contents

Executive summary

A number of previous inquiries have highlighted critical shortcomings in information sharing and recommended action including most recently, the Royal Commission into Family Violence (Royal Commission).

The Victorian Government has committed to implementing the recommendations of the Royal Commission into Family Violence, which includes recommending the creation of a specific family violence information sharing regime.

In addition to this, the Victorian Government is also considering parallel amendments to the *Privacy and Data Protection Act 2014* and *Health Records Act 2001* (default privacy legislation) that would better support information sharing in contexts beyond family violence.

As part of this work, the Department of Premier and Cabinet (the Department) is undertaking stakeholder consultation to determine whether the current exceptions to privacy protections on the basis of a serious or serious and imminent threat, which exists in default privacy legislation, should be amended.

Specifically, the Department is seeking responses to the following issues:

Exceptions to privacy protections in Victoria – the distinction between personal information and health information	
Q 1	Do the differences in the exceptions under the *Privacy and Data Protection Act 2014* (PDP Act) and the *Health Records Act 2001* (HR Act) cause difficulties for your organisation? If so, please provide any practical examples.
'Imminent' in the context of privacy legislation	
Q 2	Does your organisation ever need to collect, use or disclose personal information or health information without an individual's consent due to a serious and imminent threat?
Q 3	Does the current wording of any of the exceptions listed in Table 1 – particularly where the term 'imminent' appears - cause difficulties for your organisation?
Q 4	Should the term 'imminent' be removed as an element of existing exceptions under the PDP Act and HR Act? In all instances, or only some? Why or why not?
Preferred alternative formulation of the 'serious and imminent' exception	
Q 5	Which of the options for amending the exception set out in Table 2 does your organisation consider the most effective and appropriate?
Q 6	Are there any other options for reforming the exception that should be considered?
Q 7	What negative or unintended consequences (if any) might arise if any of the options are implemented?

Background

A number of reviews have scrutinised the interactions between privacy protections and information sharing by government and community sector organisations – most recently, in the Coronial inquest into the death of Luke Batty, the Royal Commission into Family Violence and the Royal Commission into Institutional Responses to Child Sexual Abuse.

Default privacy legislation, as established by the *Privacy and Data Protection Act 2014* (PDP Act) and *Health Records Act 2001* (HR Act), seeks to protect the privacy of individuals by regulating:

- the circumstances in which public agencies and health service providers can collect personal and health information
- the subsequent use, disclosure and management of that information.

Default privacy legislation also provides for exceptions when privacy protections can be displaced. The primary focus of this paper is the current exception, which allows organisations to displace privacy protections where there is a serious and imminent threat to an individual's life, health, safety or welfare.

The serious and imminent threshold has been criticised by previous reviews for a number of reasons – namely:

- It is difficult to apply. Determining when a threat is 'imminent' can be particularly difficult.[1]
- The requirement that a threat be 'imminent' creates an unnecessary restriction on information sharing that can make early intervention difficult. Risks are more difficult to identify and appropriate service responses cannot be implemented until the threat becomes imminent.[2]
- Information should be able to be used and disclosed where there is a serious risk of harm in the medium to long term, not only where it is imminent.[3]

The Victorian Government is keen to ensure that parallel amendments to default privacy legislation complement, as far as possible, the development of specific legislation to enable information sharing in the context of family violence and children and young people. Note that separate consultation papers are being prepared in relation to the latter.

[1] Royal Commission into Family Violence (2016) *Volume I Report and Recommendations*, 173; KPMG (2016) *Review of legislative and policy impediments to sharing relevant information between agencies in relation to a person at risk of family violence*, 22.

[2] Royal Commission into Family Violence (2016) *Volume I Report and Recommendations* 173.

[3] Australian Law Reform Commission and New South Wales Law Reform Commission (2010) *Family Violence: A National Legal Response*, 1430.

Key issues for consideration

1. Exceptions to privacy protections in Victoria – the distinction between personal and health information

Victoria's default privacy legislation regulates the collection and handling of various categories of information through two separate statutory schemes:

- the Information Privacy Principles (IPP) established under the PDP Act apply to Victorian Departments, law enforcement agencies, most statutory bodies and persons or bodies who provide services under a State contract
- the Health Privacy Principles (HPP) established under the HR Act apply to public and private organisations that provide health services in Victoria, and to other organisations that hold health information in their possession or have this information under their control.

The various categories of information regulated by default privacy legislation is listed at Appendix 1.

This distinction between the regulation of personal information and health information – also reflected to varying degrees in ACT, NSW, Queensland, South Australia and New Zealand – appears to be based on a view that health information, as a category of personal information is of significant sensitivity. The establishment of a separate scheme also reflects a view that specific health privacy protections are required to regulate the use and handling of health information by private health service providers. The distinction between the two privacy schemes may also reflect a view that a failure to protect the privacy of health information may make some individuals reluctant to seek assistance of health care providers.[4]

Exceptions to privacy protections on the basis of serious or serious and imminent threat exist in both Acts in relation to collection, use and disclosure of and access to personal and health information.

Table 1 below sets out these various formulations in Victoria's default privacy scheme.

Table 1 Serious/imminent exceptions in Victorian privacy legislation

Act or practice	Personal information	Health information	Analysis of differences
Collection			
IPP 1.5 **HPP 1.5**	Organisation is not required to advise individual about the purpose for collection or how information will be used or disclosed when collected from a third party where doing so would pose a serious threat to life or health of any individual.	No consent required if collection is necessary to prevent or lessen a serious and imminent threat to the life, health, safety or welfare of any individual, or to public health, public safety or public welfare.	HPPs make consent an express requirement of collection of health information, unless serious and imminent threat exception applies (no equivalent in IPPs).

[4] Australian Law Reform Commission (2008) *For your information: Australian Privacy Law and Practice* (ALRC Report 108) 2013.

Act or practice	Personal information	Health information	Analysis of differences
		Organisation is not required to advise individual about the purpose for collection or how information will be used or disclosed when collected from a third party where doing so would pose a serious threat to life or health of any individual.	IPPs and HPPs apply the same serious threat exception to disclosure obligations when collection information about an individual from a third party.
Use and disclosure			
IPP 2.1(d)(i) **HPP 2.2(h)(i)**	No consent required if organisation reasonably believes use or disclosure for secondary purpose is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare.	No consent required if organisation reasonably believes use or disclosure for secondary purpose is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare.	No difference.
Access			
IPP 6.1(a) **HPP 6.1(a)** **Section 26 HR Act**	Access to personal information may be refused where this would pose a serious and imminent threat to the life or health of any individual.	Access must be refused if the organisation believes on reasonable grounds it would pose a serious threat to the life or health of any individual.	IPPs allow refusal on the basis of the existence of a serious and imminent threat. HPPs require refusal on the basis of a *reasonable belief* that a serious threat exists.

Exceptions in other jurisdictions

There is no uniform standard across jurisdictions in relation to formulation of the serious and imminent exception in terms of the privacy protections governing collection, use and disclosure and access. However, the majority of jurisdictions, including New Zealand, allow organisations to use or disclose personal information and health information without consent from the relevant individual on the basis of a serious threat. The table at Appendix 2 sets out the various ways that Australian jurisdictions and New Zealand have constructed exceptions to privacy protections.

Reforms to the PDP Act and the HR Act are being considered by Government to support better information sharing in contexts beyond family violence—in particular, in relation to the 'serious and imminent' threshold contained in these two Acts.

The Department considers that it would be preferable for any proposed amendments to the exception to be consistent across both Acts, particularly where the policy basis for distinguishing the two forms of information is not applicable. The Department would be particularly interested to hear whether there is support or otherwise for more closely harmonising the exceptions under the PDP Act and HR Act.

Consultation questions:

1. Do the differences in the exceptions under the PDP Act and the HR Act cause difficulties for your organisation? If so, please provide any practical examples.

2. 'Imminent' in the context of privacy legislation

Reviews of the privacy protections in various jurisdictions, including Victoria, have found that the requirement that a threat be both serious and imminent creates a threshold that is difficult to satisfy. These reviews are:

- **Australian Law Reform Commission** (ALRC) *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108): recommended removal of the requirement that a threat be 'imminent' in the context of default privacy legislation.
- **ALRC and NSW Law Reform Commission** *Family Violence – A National Legal Response* (ALRC Report 114): recommended removal of the requirement that a threat be 'imminent' in the context of family violence specific information sharing.
- **Royal Commission into Family Violence** *Volume I: Report and Recommendations*: recommended the threshold should be a serious *or* imminent threat in the context of family violence specific legislation.
- **KPMG** *Final Report: Review of legislative and policy impediments to sharing relevant information between agencies in relation to a person at risk of family violence*: considered removal of the requirement that a threat be 'imminent' in the context of default privacy legislation.
- **Royal Commission into Institutional Responses to Child Sexual Abuse** *A study into the legislative – and related key policy and operational – frameworks for sharing information relating to child sexual abuse in institutional contexts*: noted the limitations on information sharing for preventative purposes by requiring a threat to be 'serious and imminent' in the context of child protection schemes.

Other than ALRC Report 108, the above recommendations for amending this exception appear to be confined to a family violence or child protection context, where there is a strong public interest in displacing privacy protections to protect the safety of individuals at risk of serious harm. As such, the exception may only be relevant to a small number of organisations, and within limited contexts.

The Department would be particularly interested to understand the scope of organisations that currently rely on the serious and imminent threat exception for the collection, use or disclosure of personal or health information without an individual's consent outside the family violence and child welfare or protection sector.

Consultation questions:

2. Does your organisation ever need to collect, use or disclose personal information or health information without an individual's consent due to a serious and imminent threat?

3. Does the current wording of any of the exceptions listed in Table 1 – particularly where the term 'imminent' appears - cause difficulties for your organisation?

4. Should the term 'imminent' be removed as an element of existing exceptions under the PDP Act and HR Act? In all instances, or only some? Why or why not?

3. Preferred alternative formulation of the 'serious and imminent' exception

There are a number of ways that the 'serious and imminent' threshold could be reformulated to address concerns that the current exception is not flexible enough for organisations to keep individuals safe when subject to substantial threats. Options for reform include:

- Option 1: remove the requirement that a threat be 'imminent' and require consent for the collection, use or disclosure of information unless unreasonable or impracticable to obtain (based on Commonwealth legislation).

  This would potentially complicate the existing exception by incorporating a new test for consent. While removing imminence would arguably increase information sharing, the increase would be limited by requiring consideration of whether consent is unreasonable or impracticable.

- Option 2: remove the requirement that a threat be 'imminent' with no change to consent requirements (i.e. no consent required).

  This would potentially increase information sharing compared to Option 1 by only requiring consideration of seriousness of a threat, with no further consideration of the reasonableness or practicalities of obtaining consent from the individual. Its removal would also better enable sharing of information to prevent a serious threat, which is not yet imminent, from materialising.

- Option 3: amend the exception to require that a threat be serious **or** imminent (i.e. no consent required based on the recommendation of the Royal Commission).

  This option has the greatest potential to increase information sharing, largely due to the fact that it would allow information to be shared where a threat is imminent, but not necessarily serious. For example, someone may disclose information about a person who may be the subject of insubstantial threat that is likely to occur imminently. This would be a substantial widening of the existing exception and has not been adopted in other jurisdictions.

Consultation questions:

5. Which of the options for amending the exception set out in Table 2 does your organisation consider the most effective and appropriate?

6. Are there any other options for reforming the exception that should be considered?

7. What negative or unintended consequences (if any) might arise if any of the options are implemented?

Conclusion

The Department is interested in receiving your views on the family violence information sharing legislative regime.

Written comments should be provided as soon as possible but no later than **29 August 2016** to fiona.pitman@dpc.vic.gov.au.

For further information on this project please contact:

Fiona Pitman
Senior Legal Policy Adviser
Office of the General Counsel
Department of Premier and Cabinet
1 Treasury Place
Melbourne 3002
Ph: (03) 9651 1247
fiona.pitman@dpc.vic.gov.au.

Appendix 1: Categories of information regulated by privacy legislation

Law enforcement data: any information obtained, received or held by Victoria Police for the purpose of performing law enforcement and community policing functions.

Health information: information or an opinion that is also personal information, about an individual's physical, mental or psychological health, disability, future health service provision, or health services provided, and includes genetic information.

Personal information: information or an opinion that is recorded in any form about an individual whose identity is apparent, or can be reasonably ascertained from the information or opinion.

Public sector data: any information, including personal information, that is obtained, received or held by a public sector agency or special body, whether or not the agency or body obtained, received or holds that information in connection with its functions.

Sensitive information: information or an opinion about an individual, that is also personal information, which relates to the individual's racial or ethnic origin, political opinions, membership of political associations, religious beliefs or affiliations, philosophical beliefs, membership of professional or trade associations, membership of a trade union, sexual preferences or practices, or criminal record.

Appendix 2: Use of serious and/or imminent threat as threshold in privacy legislation

Jurisdiction	Application	Personal information	Health information
Commonwealth *Privacy Act 1988* ▪ establishes the Australian Privacy Principles (APP)	Commonwealth public agencies Private organisations with more than $300 million annual turnover Health service providers – public and private	*Collection – section 16A; APP 3.4(b)* *Use – section 16A; APP 6.2(c), 9.2(d)* *Disclosure – section 16A; APP 6.2(c), 8.2(d), 9.2(d)* Consent is not required if it is unreasonable or impracticable to obtain consent, and the entity reasonably believes that the collection of personal information, or the use or disclosure of personal information for a secondary purpose, is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or public safety. Entities are not required to ensure that overseas recipients of personal information are compliant with APPs if it is unreasonable or impracticable to obtain consent, and the entity reasonably believes that the disclosure of personal information for a secondary purpose to the overseas recipient is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or public safety. *Access – APP 12.3(a)* An entity may refuse to provide an individual with access to their personal information if the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety.	Health information is defined as a subset of personal information, and is regulated by the Act and the APPs. *Use or disclosure – section 16B(4); APP 6.2(d)* ▪ Consent is not required for the use or disclosure of genetic information if it is unreasonable or impracticable to obtain consent, and ▪ the organisation has obtained the information in the course of providing a health service to the individual, and ▪ the organisation reasonably believes use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual, and ▪ the recipient of the information is a genetic relative of the first individual.

Jurisdiction	Application	Personal information	Health information
Australian Capital Territory *Information Privacy Act 2014* ▪ establishes the Territory Privacy Principles (TPP) *Health Records (Privacy and Access) Act 1997* ▪ establishes the Privacy Principles (PP)	Public sector agencies – TPPs Contracted service providers – TPPs Health service providers – public and private - PPs	*Collection – section 19; TPP 3.4(b)* *Use – section 19; TPP 6.2(c)* *Disclosure – section 19; TPP 6.2(c), 8.2(d)* Consent is not required if it is unreasonable or impracticable to obtain consent, and the agency reasonably believes that the collection of personal information, or the use or disclosure of personal information for a secondary purpose, is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or public safety. Agencies are not required to ensure that overseas recipients of personal information are compliant with APPs if it is unreasonable or impracticable to obtain consent, and the agency reasonably believes that the disclosure of personal information for a secondary purpose to the overseas recipient is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or public safety.	*Use – PP 9.1(b)* Consent is not required for the use of personal health information if the health service provider believes on reasonable grounds that use of the information for a secondary purpose is necessary to prevent or lessen a significant risk to the life or physical, mental or emotional health of the relevant individual (the consumer) or another person. *Access – section 15* A health service provider must not give access to a health record if they believe on reasonable grounds that provision of the information would constitute a significant risk to the life or the physical, mental or emotional health of the relevant individual (the consumer), or of any other person.
New South Wales *Privacy and Personal Information Protection Act 1998* ▪ establishes the Information Protection Principles (IPP) *Health Records and Information Privacy Act 2002* ▪ establishes the Health Privacy Principles (HPP)	Public sector agencies and officials – IPPs Contracted service providers – IPPs Health service providers – public and private – HPPs Organisations that collect, hold or use health information – public and private - HPPs	*Use – section 17(c)* Consent is not required for the use of personal information for a secondary purpose by an agency that holds the information if its use is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.	*Collection – HPP 4(2)(a)* When collecting information about an individual from a third party, the organisation does not need to make the individual aware of this collection if this would pose a serious threat to the life or health of any individual.

Jurisdiction	Application	Personal information	Health information
		Disclosure – section 18(1)(c), 18(2), 19(1), 19(2) Consent is not required for the disclosure of personal information for a secondary purpose if the agency that holds the information believes on reasonable grounds that disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person. An agency can only disclose personal information that is sensitive information if disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual or another person. An agency may disclose personal information to external agencies where it reasonably believes it is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person.	*Use – HPP 10(1)(c), 10(1)(c1)* *Disclosure – HPP 11(1)(c), 11(1)(c1), 14(1)(f)* Consent is not required for secondary purpose use or disclosure where the organisation reasonably believes it is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or a serious threat to public health or public safety. Consent is not required for secondary purpose use or disclosure of genetic information where the organisation reasonably believes it is necessary to lessen or prevent a serious threat to the life, health or safety (whether imminent or not) of a genetic relative of the individual. An organisation may disclose health information to external agencies where it reasonably believes it is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or a serious threat to public health or public safety. *Access – section 29(a)* A private sector person is not required to provide access to health information if this would pose a serious threat to the life or health of the individual or any other person.
Northern Territory *Information Act* ▪ establishes the Information Privacy Principles (IPP)	Public sector organisations Contract service providers	*Collection – IPP 1.5* When collecting information about an individual from a third party, the organisation does not need to take	Health information is defined as a subset of personal information, and is regulated by the Act and the IPPs. Collection, use or disclosure of health

Jurisdiction	Application	Personal information	Health information
		reasonable steps to make the individual aware of this if this would pose a serious threat to the life or health of the individual or another individual. *Use or disclosure – IPP 2.1(d)* Consent is not required for use or disclosure for a secondary purpose where the organisation reasonably believes it is necessary to lessen or prevent a serious and imminent threat to the individual's or another individual's life, health or safety, or a serious and imminent threat to public health or public safety. *Access – IPP 6.1(a)* An organisation is not required to provide an individual with access to their information if providing access would pose a serious threat to the life or health of the individual or another individual.	information is not specifically differentiated in relation to an exception to consent requirements to manage threats to an individual.
Queensland *Information Privacy Act 2009* ▪ establishes the Information Privacy Principles (IPP) and the National Privacy Principles (NPP)	Ministers Departments Local governments - IPPs Public authorities - IPPs Contracted service providers – IPPs Health agencies – public and private - NPPs	*Use – IPP 10(1)(b)* Consent is not required for use of information for a secondary purpose if an agency is satisfied on reasonable grounds that the use is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare. *Disclosure – section 33, IPP 11(1)(c)* An agency may disclose information if satisfied on reasonable grounds that disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or	*Collection – NPP 1(5)(b), 9(1)(c)* Consent is not required for collection of sensitive information if it is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of an individual, and the relevant individual cannot give consent. A health agency is not required to make an individual aware that information about them has been collected from a third party if making the individual aware would pose a serious threat to the life, health, safety or welfare of an individual. *Use or disclosure – NPP 2(1)(d)* Consent is not required

Jurisdiction	Application	Personal information	Health information
		welfare. An agency may transfer information to an entity outside Australia if it is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare.	for use or disclosure of information for a secondary purpose if a health agency reasonably believes that it is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare, or to public health, safety or welfare.
South Australia *Information Privacy Principles Instruction* ▪ establishes the Information Privacy Principles (IPP) *Health Care Act 2008* (HCA)	Public sector agencies Contracted service providers Health service providers – public and private	*Use or disclosure – IPP (8)(c)* Consent is not required for use or disclosure for a secondary purpose if the agency believes on reasonable grounds that it is necessary to prevent or lessen a serious threat to the life, health or safety of the individual or some other person.	*Disclosure – section 93(3)(e) HCA* Consent is not required for disclosure for a secondary purposes if this is reasonably required to lessen or prevent a serious threat to the life, health or safety of a person, or a serious threat to public health or safety.
Tasmania *Personal Information Protection Act 2004* ▪ establishes the Personal Information Protection Principles (PIPP)	Public authorities Contracted service providers Health service providers – public and private	*Collection – PIPP 1(5), 10(1)(c)* When collecting information about an individual from a third party, the authority does not need to take reasonable steps to make the individual aware of this if this would pose a serious threat to the life, health or welfare of any individual. Consent is not required for collection of sensitive information if it is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of an individual, and the relevant individual cannot give consent. *Use or disclosure – PIPP 2(1)(d)* Consent is not required for use or disclosure for a secondary purpose if the authority reasonably believes is necessary to lessen or prevent a serious threat to an	Health information is defined as a subset of personal information, and is regulated by the Act and the PIPPs. Collection, use or disclosure of health information is not specifically differentiated in relation to an exception to consent requirements to manage threats to an individual.

Jurisdiction	Application	Personal information	Health information
		individual's life, health, safety or welfare, or to public health or public safety.	
Victoria *Privacy and Data Protection Act 2014* ▪ establishes the Information Privacy Principles (IPP) *Health Records Act 2001* ▪ establishes the Health Privacy Principles (HPP)	Public sector agencies – IPPs Contracted service providers – IPPs Health service providers – public and private – HPPs	*Collection – IPP 1.5* When collecting information about an individual from a third party, an organisation does not need to take reasonable steps to make the individual aware of this if this would pose a serious threat to the life or health of any individual. Consent is not required for collection of sensitive information if it is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, and the relevant individual cannot give consent. *Use or disclosure – IPP 2.1(d)* Consent is not required for use or disclosure for a secondary purpose if the organisation reasonably believes it is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare, or to public health, public safety or public welfare. *Access – IPP 6.1(a)* An organisation may refuse to provide an individual with access to their personal information if it would pose a serious and imminent threat to the life or health of any individual.	*Collection – HPP 1.1(f), 1.5* Consent is not required for the collection of health information if it is necessary to prevent or lessen a serious and imminent threat to the life, health, safety or welfare of any individual, or to public health, public safety or public welfare. When collecting health information about an individual from a third party, an organisation does not need to take reasonable steps to make the individual aware of this if this would pose a serious threat to the life or health of any individual. *Use or disclosure – HPP 2.2(h)* Consent is not required for use or disclosure for a secondary purpose if the organisation reasonably believes it is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare, or to public health, public safety or public welfare. *Access – section 26, HPP 6.1(a)* An organisation must not give an individual access to their health information if it believes on reasonable grounds that to do so would pose a serious threat to the life or health of the individual or any other person.
Western Australia *Freedom of Information Act 1992* (FOI Act)	Western Australia does not regulate privacy through legislation, other than to provide some restrictions on disclosure of personal information under its freedom of information scheme where the individual to whom the information relates does not consent to its disclosure. The FOI Act does not set out any test for waiving of consent on the grounds of a threat to an individual.		

Jurisdiction	Application	Personal information	Health information
New Zealand *Privacy Act 1993* ▪ establishes the Information Privacy Principles (IPP) *Health Information Privacy Code 1994* ▪ establishes the Health Information Privacy Rules (HIPR)	Agencies – public and private – IPPs Health and disability service providers – HIPRs	*Use – IPP 10(d)* Consent is not required for use of information for a secondary purpose if the agency reasonably believes it is necessary to lessen or prevent a serious threat to public health or public safety, or to the life or health of the individual concerned or another individual. *Disclosure – IPP 11(f)* Consent is not required for use of information for a secondary purpose if the agency reasonably believes it is necessary to lessen or prevent a serious threat to public health or public safety, or to the life or health of the individual concerned or another individual.	*Use – HIPR 10(1)(d)* Consent is not required for use of information for a secondary purpose if the agency reasonably believes it is necessary to lessen or prevent a serious threat to public health or public safety, or to the life or health of the individual concerned or another individual. *Disclosure – HIPR 11(2)(d)* Consent is not required for disclosure of information for a secondary purpose if the agency reasonably believes it is necessary to lessen or prevent a serious threat to public health or public safety, or to the life or health of the individual concerned or another individual.