Introduction

The *Family Violence Protection Amendment (Information Sharing) Act 2017* (**the Amending Act**) establishes an information sharing scheme by amending the *Family Violence Protection Act 2008* and other laws, including the *Privacy and Data Protection Act 2014* (PDPA) and the *Health Records Act 2001* (HRA).

One of the key changes to the PDPA and the HRA is the removal of the word ‘imminent’ from several provisions in the Information Privacy Principles (IPPs) and the Health Privacy Principles (HPPs).[[1]](#footnote-1) These provisions previously referred to a ‘serious and imminent threat’, which was the threshold that, if established, permitted the collection, use and disclosure of an individual’s personal and health information in order to lessen or prevent the threat.

The purpose of this document is to provide an overview of this change and offer guidance for organisations as to the considerations that may be relevant to determining what is a ‘serious’ threat. While the PDPA and the HRA contain different obligations for personal information and health information, this guidance addresses the removal of ‘imminent’ in relation to both the IPPs and the HPPs.[[2]](#footnote-2)

Background

Discussion around removing ‘imminent’ from the ‘serious and imminent threat’ exception has been ongoing for a number years, and was raised by the Australian Law Reform Commission (ALRC) as early as 2008.[[3]](#footnote-3) In Victoria, the impetus for legislative change to remove ‘imminent’ resulted from the Royal Commission into Family Violence (RCFV) in 2015.

In its final report, the RCFV noted that:

*Many family violence cases will not meet this threshold. This is because requiring the threat to be both ‘serious’ and ‘imminent’ sets a high bar. In particular, whether a threat is ‘imminent’ can be uncertain and difficult to establish in the dynamic context of family violence. In addition, while the evidence of ‘imminence’ may be unclear, the threat can nevertheless be serious and a victim placed at real risk.*[[4]](#footnote-4)

While the legislative change in Victoria came about in the context of family violence prevention, the removal of ‘imminent’ from the IPPs and the HPPs has a broader application beyond family violence.

Removing ‘imminent’ – the legislative change

Sections 19 and 22 of the Amending Act amend both the PDPA and the HRA to remove the word ‘imminent’ from the ‘serious and imminent threat’ exception, requiring that a threat need only be ‘serious’. Each of the principles and their amendment are discussed in turn below.

HPP 1.1(f)(i) – Collection of health information

When an organisation seeks to collect health information about an individual, the collection must be necessary for one or more of its functions or activities. It must also meet one of the provisions under HPP 1.1. Under the amendment to HPP 1.1(f)(i), an organisation may collect health information if it is ‘necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual’. By removing ‘imminent’, organisations may now collect health information under HPP 1.1(f)(i) if there is a ‘serious’ threat that can be lessened or prevented through the collection of that information.

A client of a health service is behaving aggressively and has made threats towards staff. The health service manager is considering whether to exclude the person from attending the health service in the future. The manager is aware that the client also receives services from another organisation, and is considering contacting the other organisation to seek information about the client that may justify excluding him from attending the health service. Previously, the manager may not have been able to collect the client’s health information from the other organisation unless the threat was expected to be carried out in the immediate future. Now, the manager can collect the information if the threat is serious and staff are at risk, even if the timing of a possible future incident is unknown.

IPP 2.1(d)(i) and HPP 2.2(h)(i) – Use and Disclosure of personal and health information

IPP 2 and HPP 2 state that personal and health information should only be used or disclosed for the primary purpose for which the information was originally collected, unless a permitted exception applies.

The exceptions include IPP 2.1(d)(i) and HPP 2.2(h)(i), which, in the amended form, permit a organisation to use or disclose personal or health information for a secondary purpose if it reasonably believes that doing so is necessary to ‘lessen or prevent a serious threat to an individual’s life, health, safety or welfare’.

The removal of ‘imminent’ means that to now share personal or health information under this exception, an organisation need only establish that a threat to an individual is ‘serious’, but not necessarily ‘imminent’.

IPP 2.1(d)(ii) and HPP 2.2(h)(ii) have always provided that where there is a threat to the health, safety or welfare of the public, the threat need only be ‘serious’ for use and disclosure of personal or health information to be permissible. Therefore, this change streamlines when an organisation can use or disclose personal or health information where there is a serious threat to individuals or the public, eliminating potential confusion between these provisions.

A patient was discharged from hospital after receiving mental health treatment. The patient then attends a police station and files a report about the way another patient treated her in hospital. In making the complaint, the patient becomes upset and admits that she had suicidal thoughts and self-harmed. The police officer contacts a mental health worker at the hospital to express concern for the woman’s safety, believing that she may try to harm herself again. Even though the police officer could not predict when the woman may next self-harm, the officer is able to lawfully contact the hospital given the nature of the possible harm is serious enough to put the woman’s life at risk.

IPP 6.1(a) – Access to personal information

IPP 6 provides individuals with a right to access and correct their personal information. IPP 6 is designed to complement Victoria’s freedom of information scheme. It ensures that the right to access and correction of documents in the possession of government is maintained for public sector organisations that are not subject to the *Freedom of Information Act 1982* (Vic) (FOI Act) (typically contracted service providers).

IPP 6.1(a) provides an exception to the obligation to give access to, or correct, personal information, where an organisation can establish that ‘providing access would pose a serious threat to the life or health of any individual.’ The removal of ‘imminent’ from this provision means that organisations not subject to the FOI Act can refuse to provide access to personal information held about an individual if doing so would pose a serious threat to the life or health of any individual, regardless of whether or not the timing of any incident is imminent.

IPP 10.1(c) – Sensitive Information

Due to its nature, sensitive informationattracts increased protections under IPP 10 in terms of when this type of information can be collected.[[5]](#footnote-5)

An organisation must not collect sensitive information about an individual unless they have consented, or one of the other permissible exceptions under IPP 10.1 applies.

Under IPP 10.1(c), an organisation may collect sensitive information if it is ‘necessary to prevent or lessen a serious threat to the life or health of any individual’, and the individual is physically or legally incapable of giving consent to the collection. As with other provisions, the removal of ‘imminent’ lowers the threshold that an organisation must meet in order to collect sensitive information.

Why is this change important?

The overarching purpose of the removal of ‘imminent’ from the ‘serious and imminent threat’ exception is to lower the threshold to permit information sharing in situations where there may be a threat that is ‘serious’, but not necessarily ‘imminent’.

This amendment means Victorian public sector organisations are able to broaden their ability to assist individuals in situations where there is a reasonable belief that a threat is ‘serious’. It also enables preventative measures to be taken where a threat is established, beforea risk escalates further.

The removal of ‘imminent’ does not diminish the importance of information privacy, but instead realigns the balance between the protection of privacy and the free flow of information. As a result of this change, frontline workers such as police officers, social workers and child protection case managers can take a more proactive and dynamic approach to assessing and managing the seriousness of a threat.

The ‘serious’ test

Whether or not a threat can be considered ‘serious’ for the purposes of the PDPA and the HRA should take into account what a reasonable person would regard as ‘serious’. The ALRC proposed that an assessment of whether a threat is ‘serious’ should involve a consideration of the gravity of the potential outcome as well asits relative likelihood.[[6]](#footnote-6)

In making an assessment as to whether a threat is ‘serious’ under the IPPs and HPPs, organisations should consider the following factors:

* **Severity -** *How significant are the consequences of the threat?*
* **Likelihood** - *What is the chance of the threat actually happening? What is the relative likelihood that harm will occur?*

There are a range of other circumstances that may impact upon the seriousness of a threat. It may not be clear in all situations whether a threat is likely to ever happen or how severe the consequences might be for an affected individual. In these cases, organisations may wish to look at secondary factors applicable to the particular situation in making an assessment as to the severity and likelihood of the threat.

These factors may include, but are not limited to:

* **Timing -** *How soon is the threat likely to occur? Is the threat ongoing?*
* **Nature of the harm -** *What is the level of**perceived harm to the individual? What type of harm is likely to result (e.g. physical, mental, financial)?*
* **Vulnerability -** *Considering the circumstances, how vulnerable might the affected individual be to the threat (e.g. is the victim a child?)*

These secondary factors may not be relevant in every case, but in some situations, may assist in making an assessment as to whether a threat is ‘serious’. Seriousness should be determined on a case by case basis, as the circumstances surrounding a threat will differ.

Removing ‘imminent’ from the threshold increases the degree of flexibility afforded to organisations seeking to collect, use or disclose personal and health information. Even where a ‘serious’ threat has been established, organisations still need to consider if sharing the information is necessaryto prevent or lessen a threat, including whether the recipient is in a position to act on the information.8

A prisoner is attending a medical appointment. He tells the nurse that the first thing he is going to do when he is released is hunt down his former partner and make her pay for telling his family that he has HIV. The nurse believes that this threat is serious as the prisoner is implying that he is going to harm his former partner. However, the nurse is unaware of when the prisoner will be released from prison, and as such the threat may not be immediate. The fact that the prisoner may not be released from prison for some time will not prevent the nurse from disclosing this information to the relevant officers in the prison system, as the threat could potentially be severe enough to risk his former partner’s life, and the probability of it occurring once the prisoner is released is high.

Further Information

**Victorian Information Commissioner**

**t:** 1300 00 6842
**e:** enquiries@ovic.vic.gov.au
**w:** ovic.vic.gov.au**Health Complaints Commissioner**

**t:** 1300 582 113
**e:** hcc@hcc.vic.gov.au
**w:** hcc.vic.gov.au

Please note that the contents above are for general information purposes only, and should not be relied upon as legal advice. OVIC and HCC do not guarantee or accept legal liability whatsoever arising from, or connected to the accuracy and reliability of the contents of this information.[[7]](#footnote-7)

1. Specifically, IPPs 2.1(d), 6.1(a) and 10.1(c), and HPPs 1.1(f) and 2.2(h). [↑](#footnote-ref-1)
2. While this guidance offers an overview incorporating both personal information and health information, public sector organisations should be aware of the type of information they are handling, and the considerations they need to make under both the PDPA and the HRA. [↑](#footnote-ref-2)
3. Section 72 – Exceptions to the Use and Disclosure Offences, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108),* August 2008, and Section 30 – Information Sharing, *Family Violence – A National Legal Response (ALRC Report 114)*, November 2014. [↑](#footnote-ref-3)
4. *Royal Commission into Family Violence Report and Recommendations*, March 2016*,* Volume 1, Chapter 7, page 173. [↑](#footnote-ref-4)
5. Sensitive information is a subtype of personal information and is specifically defined in Schedule 1 of the PDPA. It includes racial or ethnic origin, political opinions and associations, religious or philosophical beliefs, membership of trade associations or unions, sexual preferences or practices, and criminal record. [↑](#footnote-ref-5)
6. *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108), August 2008, Point 25.72. [↑](#footnote-ref-6)
7. *Guidelines to the Information Privacy Principles*, 2011, page 64. [↑](#footnote-ref-7)