

APRIL 2025

Guidance on Adopting Model Legislative Provisions

Information sharing and
confidentiality

The Secretary
Department of Treasury and Finance
1 Treasury Place
Melbourne Victoria 3002
Australia
Telephone: +61 3 9651 5111
dtf.vic.gov.au

Authorised by the Victorian Government
1 Treasury Place, Melbourne, 3002

© State of Victoria 2025



You are free to re-use this work under a [Creative Commons Attribution 4.0 licence](#), provided you credit the State of Victoria (Department of Treasury and Finance) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any branding, including Government logos.

If you have copyright queries or would like to receive this publication in an accessible format email information@dtf.vic.gov.au

ISBN 978-1-923295-06-3 (pdf/online/MS word)
Published April 2025

This document is available in Word and PDF format at dtf.vic.gov.au

Contents

1.	Background	1
1.1	Confidentiality and information sharing	1
1.2	Adopting the model provisions	5
1.3	Structure of this document	7
2.	What kind of information is being disclosed?	7
2.1	Personal information	8
2.2	Health information	9
2.3	<i>Victorian Data Sharing Act 2017</i>	10
3.	Sharing related to Department and regulator functions	11
3.1	Category 1: General permission to share	15
3.2	Category 2: Permission to share with limited restrictions	21
3.3	Category 3: Permission to share with substantial restrictions	26
3.4	Category 4: Obligation of confidentiality with some limited permissions to share	27
3.5	Category 5: General obligation of confidentiality	30
	Appendix A – Consolidated Model Provisions provided by OCPC	32
	Appendix B – Consolidated list of resources	40

How this document helps you

This document has been written for legislative and policy officers working with the Office of the Chief Parliamentary Counsel (OCPC) on new or amended legislative provisions in regulatory schemes.

The Department of Treasury and Finance (DTF) has prepared this document in collaboration with OCPC and in close consultation with departments and regulators. This document does not provide a 'one size fits all' or mandated approach, but guides policymakers through the conceptual and legislative considerations to make it easier to develop legislative provisions suited to your needs and aligned with best practice.

DTF has consulted OCPC and OCPC has drafted a clause bank of Model Legislative Provisions. These reflect the most modern and effective version of a regulatory provision, align with best practice, and promote consistency across Victoria's regulatory environments.

Context

Victoria has over 60 state government regulators with responsibility for over 500 different permission schemes (licences, permits and other approvals which grant the recipient permission to conduct an activity, operation or establish a premises that would otherwise be unlawful).

Legislation governing Victoria's regulators varies significantly in provisions covering the same topic. Some variations are justified and reflect the different needs of regulators and regulated entities, as well as the level and likelihood of harm being managed. However, many of these are needless, create confusion for regulators, frustration for businesses and detract from the effectiveness and efficiency of the overall regulatory system.

This model provisions guidance helps you to prepare, at the policy development stage, for your discussions with OCPC on confidentiality and information sharing activities. This guidance complements the following guides that should be considered before you conduct your review of your regulatory scheme:

- Office of the Victorian Information Commissioner's (OVIC): Guidance on information sharing and privacy, which offers some practice guidance for public sector organisations on sharing personal information.
- Delegations Guidance Note: This document supports policymakers in identifying powers which may be appropriate for delegation, as well as the scope of the delegation (broad or narrow). The Guidance Note should be read concurrently with this document.

This model provisions guidance forms part of a series of model provisions guidance covering:

- fit and proper person tests
- inspector and entry powers and regulator toolkits
- authorised officer appointments, service of documents, and commencing legal proceedings.

Adoption of model provisions is not compulsory, but they are a helpful tool for legislative policy areas seeking to introduce or revise legislation.

If you are working with a national scheme, alignment with the national scheme is often a paramount consideration to maximise the benefits and efficiencies from harmonised approaches. However, where there is scope to tailor provisions or where your input is sought on new or amended provisions, the considerations in this guidance will also be useful conceptual tools.

1. Background

1.1 Confidentiality and information sharing

Responsible information sharing can significantly benefit the Government and community. It can reduce the number of touch points between business and the Government and enable more efficient service delivery. In some circumstances there is a need to proactively share information between regulators, and between regulators and integrity law enforcement agencies, e.g. where non-compliance with one Act might be highly indicative of non-compliance with another Act, and regulators may miss key risks due to inadequate coordination with other agencies. At other times, sharing certain information with individuals, regulated entities or the public may achieve other public policy objectives, such as helping adoptees and their natural relatives to reconnect.

An organisation's ability to share information may depend on:

- whether authority to share is contained in the organisation's enabling legislation
- whether authority to share is contained in specific information sharing or privacy laws
- other non-legislative factors, such as whether an information sharing culture exists within a particular organisation.

The category of information which an organisation is seeking to share (or keep confidential), such as personal or health information, will also give rise to different restrictions and permissions.

This document contains model provisions for sharing information related to department and regulatory functions (see section 3).

Application of general legislation

Policymakers should consider how general legislation affects whether and how information can be shared. This includes, for example, legislation regulating the disclosure and use of personal information and health information, and legislation relevant to human rights (see below).

Legislation	Summary
<i>Victorian Data Sharing Act 2017</i>	Allows data sharing between government departments and agencies (not with community organisations or businesses) for the approved purpose of 'policy making and service planning and design' (not for targeting services or regulatory activities for individuals).
<i>Privacy and Data Protection Act 2014</i>	<p>Provides for the responsible handling of personal information in the Victorian public sector, while balancing the flow of information.</p> <p>Sets out ten Information Privacy Principles (IPPs), which form the general parameters for information sharing. The IPPs are categorised as follows:</p> <ul style="list-style-type: none">• Collection• Use and disclosure• Data quality• Data security• Openness• Access and correction• Unique identifiers• Anonymity• Transborder data flows• Sensitive information. <p>The full text of the IPPs can be found in Schedule 1 to the <i>Privacy and Data Protection Act 2014</i> here.</p> <p>Part 4 of the Act also provides for the Victorian Protective Data Security Standards (VPDSS), which set 12 high-level requirements for protecting public service information (which includes personal information).</p> <p>Public sector organisations subject to Part 4 of this Act must comply with the VPDSS. Detailed information on the VPDSS is available on the OVIC website here.</p>

Legislation	Summary
<i>Health Records Act 2001</i>	<p>Applies to the collection, use and handling of identifying personal information defined as 'health information' under the <i>Health Records Act 2001</i>.</p> <p>Establishes 11 Health Privacy Principles (HPPs) that apply to health information collected and handled in Victoria by the Victorian public sector and the private sector. The HPPs are categorised as follows:</p> <ul style="list-style-type: none"> • Collection • Use and disclosure • Data quality • Data security and retention • Openness • Access and correction • Identifiers • Anonymity • Transborder data flows • Transfer or closure of the practice of a health service provider • Making information available to another health service provider. <p>The full text of the HPPs can be found in Schedule 1 to the Health Records Act 2001 (Vic).</p>
<i>Charter of Human Rights and Responsibilities Act 2006</i>	<p>Sets out the protected rights, responsibilities and freedoms of Victorians, and requires that all bills proposed in Victorian Parliament be accompanied by a statement of compatibility (section 28).</p> <p>Relevant rights include, for example, a right to privacy (see section 13) which may be relevant where a person's information is collected or used.</p>
<i>Data Availability and Transparency Act 2022 (Cth)</i>	<p>Establishes a scheme where Commonwealth bodies are authorised to share their public sector data with Accredited Users (who are authorised to collect and use the data – where the requirements of the Act are met), which include state government bodies.</p> <p>State government bodies may also be Accredited Data Service Providers, who can provide complex data integration, de-identification and secure data access services.</p>
<i>Privacy Act 1988 (Cth)</i>	<p>Regulates the handling of personal information for captured entities (which does not, in general, include state government bodies, except for Acts and practices related to My Health Records, individual healthcare identifiers, and entities prescribed by the Privacy Regulation 2013).</p>
<i>Spent Convictions Act 2021</i>	<p>Establishes a scheme which limits the disclosure of spent convictions information and creates an offence for sharing spent conviction information where it is not authorised by the Act or Regulations.</p> <p>Further information is available on the Department of Justice and Community Safety website.</p>

The general application of these regimes should be considered closely when adopting model provisions to ensure compliance with all relevant requirements, noting that some of these regimes apply only when handling personal information.

When sharing information, including highly classified data, between organisations, agencies should also consider the [Victorian Protective Data Security Framework](#). This includes considering the level of assurance needed between groups to ensure that shared data can be managed and stored in lien with data classification requirements and criticality.

Identifying information for sharing

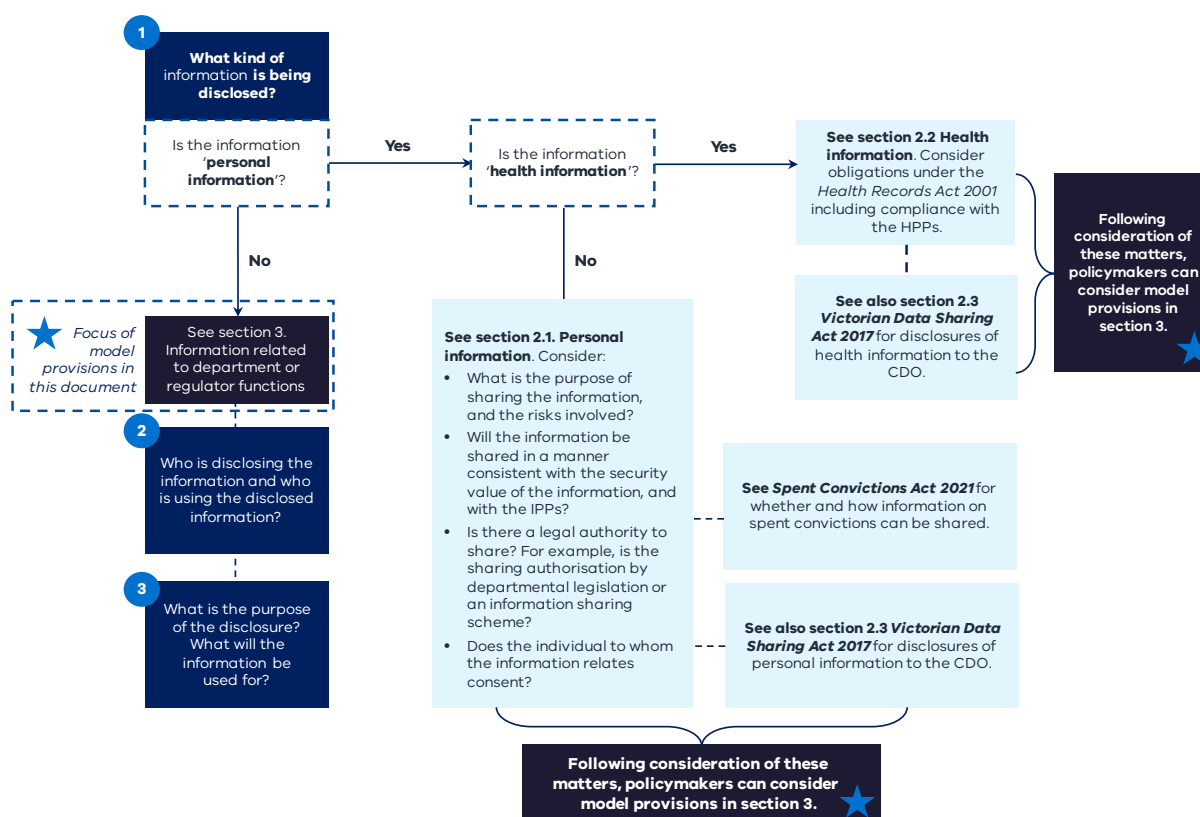
Before considering the application of model provisions and engaging in information sharing activities, policymakers should consider key questions to determine whether sharing may be permitted under Victoria’s existing legislative frameworks (including those regimes outlined above).

These questions include:

- **What kind of information is being disclosed?**
- **Who is disclosing the information and who is using the disclosed information?**
- **What is the purpose of the disclosure? What will the information be used for?**

The following sections will consider these questions further.

As shown in the diagram below, information related to department and regulatory functions may, in some cases, also be personal or present health information. Where this is the case, policymakers must consider the additional regulations described in section 3 before sharing these categories of information.



1.2 Development of Model Provisions

There are established and broadly accepted best practice principles for legislative development and drafting. These principles are reflected in various Victorian Government guidance documents and underpin the provisions and guidance in this document (see below).

Table 1: Application of best practice legislative drafting principles

Principle	Overview	Application to confidentiality and information sharing
Clear purpose	<p>Departments should consider the need to regulate before doing so. Better Regulation Victoria's principles for good regulatory practice can help ensure regulators are clear on the desired regulatory outcome and the harms which they are seeking to minimise.</p>	<p>Policymakers should first consider if a regulator can rely on general laws before considering the need for a specific provision on information sharing in a regulator's primary Act.</p> <p>Model provisions should adopt a presumption or starting point in favour of sharing unless there are compelling reasons otherwise.</p> <p>Model provisions might also identify general prohibitions, with guidance that supports regulators in identifying where a prohibition on sharing or an obligation of confidentiality should be applied.</p>
Plain language drafting and streamlined structure	<p>Clear and concise drafting, using plain language, helps reduce complexity. This ensures provisions are user-friendly and the meaning (and implications) of the text is clear.</p> <p>This means prioritising the most important concepts and leaving those not required to be contained in a principal Act for inclusion in a subordinate instrument (such as regulations).</p> <p>In the compliance context, plain legislative language and a streamlined structure facilitates the coordination of staff and cooperation between regulators.</p>	<p>Model provisions should adopt consistent language (with supporting guidance encouraging regulators to similarly adopt such language) to remove ambiguity.</p> <p>Model provisions should reflect a streamlined structure where principal Acts contain the most important elements and requirements for sharing (i.e. that sharing of information, or classes of information is permitted).</p> <p>Detail on the mechanics of how information may be shared (including sharing to classes of persons, entities or government bodies) may be best contained in subsidiary instruments to support ease of amendment.</p>

Principle	Overview	Application to confidentiality and information sharing
Proportionate	<p>Legislation should only create a regulatory burden or impost proportionate to the harm the legislation is seeking to prevent.</p> <p>The Victorian <i>Charter of Human Rights and Responsibilities Act 2006</i> requires the Victorian Government, local councils and other public authorities to assess compatibility with human rights when creating legislation, implementing policies or delivering services - an additional proportionality consideration.</p> <p>In line with the Victorian Government's Regulatory Reform Program, legislation should focus on reducing the regulatory burden it places on businesses, government, and the community.</p>	<p>Model provisions should balance personal privacy and public interest considerations in transparency, while also realising efficiencies and improvements for business, government or community efficiencies which can be gained through sharing.</p>
Objective and future-proofed	<p>Legislation should be drafted to be technology neutral and avoid any specific requirements which might lose relevance over time.</p>	<p>Model provisions should be technology agnostic.</p> <p>This will allow regulators, where appropriate, to share information using technology or on an automated basis in low-risk scenarios, and leverage technological solutions, such as the Service Victoria Identity Verification Service.</p>

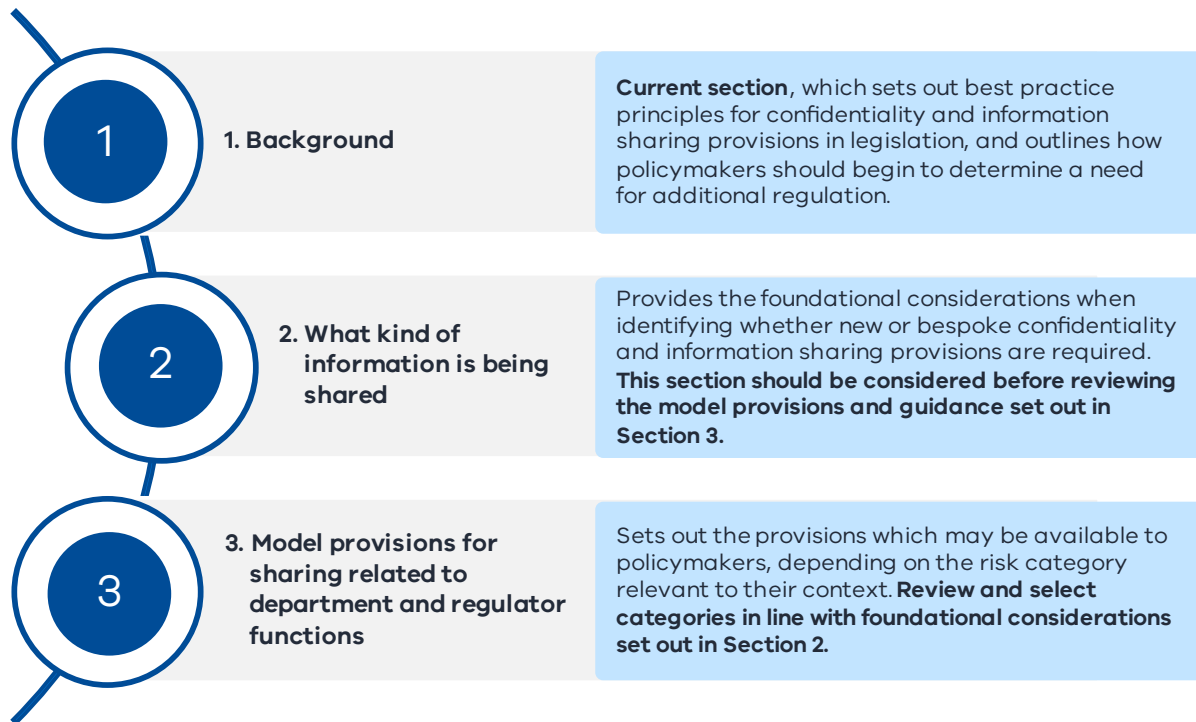
In addition to forming a basis for model provisions, policymakers are encouraged to use these principles to identify and justify the clauses which may be most appropriate for their specific legislation.

Note: This document has been designed to cater to a range of risk and regulatory environments. However, in some circumstances regulators will require a tailored provision to address the harms they are seeking to mitigate. This should occur through engagement with the Office of the Victorian Information Commissioner, relevant departments and OCPC.

Policymakers should also consider OCPC's [Legislative Process handbook](#).

1.3 Structure of this document

This document is designed to be read sequentially, in line with the below diagram. Section 2 *What kind of information is being disclosed* should be considered before model provisions in section 3.



2. What kind of information is being disclosed?

The nature and sensitivity of information determines whether and how the information is permitted to be disclosed or used by a government agency. For example, additional legislation may apply to personal and health information to protect the privacy of individuals.

The following guidance should be read in conjunction with OVIC's flowchart to support decision making, **see OVIC's website**.

2.1 Personal information

Before sharing personal information, consider the following questions: 

- What is the purpose of sharing the information?
- What are the risks involved?
- Will the information be shared in a manner consistent with the:
 - security value of the information
 - IPPs?
- Is there a legal authority to share? For example, is the sharing authorisation by departmental legislation or an information sharing scheme authorised by legislation?
- Has the individual to whom the information relates provided valid consent? For more information on consent, refer to the 'Key Concepts' chapter of OVIC's [IPP Guidelines](#).

In Victoria, the *Privacy and Data Protection Act 2014* (PDPA) regulates the handling of 'personal information'. Section 3 of the PDPA defines 'personal information' as:

'Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion but does not include information of a kind to which the Health Records Act 2001 (Vic) applies.'

The PDPA also establishes 10 Information Privacy Principles (IPPs) which form the general parameters for information sharing. The IPPs apply to all personal information, including personal information held by Victorian Government departments and agencies. Any legislation regulating the collection, use, disclosure or other handling of personal information should operate and be interpreted in harmony with the IPPs as far as possible.

There is a history of established case law in Victoria which has developed this approach to personal information. For example, in *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, Bell J noted at [61]:

'In the process of interpretation, I would take into account that the [IPPs] are intended to operate in a practical and sensible way so as to afford privacy protection to personal information held by Victorian governmental organisations. In that process, the operation of principles expressed more generally should not be restricted and the operation of principles expressed more specifically should not be diluted.'

Section 6(1) of the PDPA relates to the Act's relationship with other laws:

If a provision made by or under this Act (other than Division 5, 6 or 7 of Part 3) relating to an Information Privacy Principle or applicable code of practice is inconsistent with a provision made by or under any other Act, that other provision prevails and the provision made by or under this Act is (to the extent of the inconsistency) of no force or effect.

However, the Victorian Supreme Court has recognised a strong presumption that the IPPs operate alongside the legislation of a department or agency and should be read harmoniously with other applicable legislation. In *McLean v Racing Victoria Ltd* [2019] VSC 690, Richards J held at [57]:

'There is a strong presumption that Parliament does not intend to contradict itself, and intended that both Acts should operate. That intention is evident from the Explanatory Memorandum for the Privacy and Data Protection Bill 2014, which explained that clause 6 would 'allow relevant aspects of the IPPs to overlay the operation of other Acts where requirements can be observed concurrently'. The two Acts should therefore be read harmoniously if possible.'

For more information on the PDPA, including the operation of the IPPs and related privacy obligations, [see OVIC's website](#).

The model provisions have been developed with general laws on privacy in mind. When making or amending legislation (including adopting model provisions), policymakers should generally avoid displacing, duplicating, or unduly limiting general privacy laws unless there is a clear rationale for seeking to do so.

2.2 Health information

Before sharing health information, consider obligations under the *Health Records Act 2001*, including compliance with the HPPs.



In Victoria, the *Health Records Act 2001* (HR Act) regulates the health information of individuals, including collection and handling. Section 3 of the HR Act defines '**health information**'. This includes, among other things:

'(a) information or an opinion about –

- (i) The physical, mental or psychological health (at any time) of an individual;*
- (ii) A disability (of any time) of an individual;*
- (iii) An individual's expressed wishes about the future provision of health services to him or her; or*
- (iv) A health service provided, or to be provided to an individual –*

that is also personal information.'

Section 3 of the HR Act also provides that health information includes other personal information collected in the provision of a health service, collected in connection with the donation or intended donation of an individual's organs, and other genetic information which could be predictive of an individual's health.

The Act also establishes eleven Health Privacy Principles (HPPs) which apply to health information collected and handled in Victoria.

For more information on the HR Act, including obligations and restrictions on sharing health information, see the [Department of Health website](#).

2.3 *Victorian Data Sharing Act 2017*

Consider how the Victorian Data Sharing Act 2017 may allow for disclosures of personal information and health information with the Victorian Chief Data Officer (CDO) on request.



The *Victorian Data Sharing Act 2017* (VDS Act) permits information and data sharing between government departments to improve policies and enhance service delivery for the public interest. The VDS Act creates a framework for information sharing related to policy making, service planning and design, with the oversight of the Victorian CDO.

The VDS Act designates certain organisations as 'data sharing bodies', permitting them to share:

- personal and health information with the CDO on request and with data analytics bodies
- data that is subject to secrecy provisions when requested by the CDO.

Under the Act, data sharing bodies must:

- after receiving a request, respond by either providing the data or information or providing reasons for refusing the request
- let the CDO know if providing data knows that is subject to a 'secrecy provision'.

For more information on the operation and application of the VDS Act, see the [Victorian Government's guide for departments and agencies](#).

3. Sharing related to Department and regulator functions

Model provisions contained in this section relate to information used or disclosed in connection with the functions of departments or regulators (collectively referred to in this section as 'agencies'). This may include, for example:

- **business information and data** collected by agencies in the course of business registrations, licensing and permission applications
- **compliance information and data** which may be collected by agencies to understand a regulated entity's compliance with applicable legislative frameworks, and take action for non-compliance
- **other information collected, used or disclosed in the course of an agency's functions.** For example, under the *Adoption Act 1984*, the Secretary may use and disclose adoption information. This use and disclosure would be considered a sharing activity relating to department and regulator functions. Other examples might relate to verifying the identity of an individual, which is likely to have elements of personal information.

The above categories of information may also be, in some cases, personal or health information. Where this is the case, policymakers must consider the additional regulations applying to these categories of information (set out in section 2 of this document) before adopting and applying model provisions.

Consider if desired sharing activities are already permitted

Where sharing is not restricted by other legislation, the HPPs and IPPs form the general parameters for permitted sharing activities. This means that where sharing of information related to department and regulatory functions is consistent with the HPPs and IPPs, it is already permissible under general laws – without developing agency-specific information sharing provisions.

In most cases, agencies should not require an express legislative provision to support information sharing. However, agencies may desire express provisions in their legislation to support or constrain information sharing where the department's operating context is particularly unique, or where there is stakeholder sensitivity about information and desire for greater clarity, transparency and confidence.

Approaches to information sharing and confidentiality

Legislative provisions take varied approaches to information sharing and confidentiality. These approaches reflect:

- the risks and harms which policymakers seek to mitigate
- the circumstances in which they might be applied
- an agency's information sharing culture and maturity.

The table below identifies five categories of information sharing and confidentiality provisions, which reflect best practice. These categories form the basis of the model provisions set out in this section.



Clear purpose in practice

Before adopting model provisions in one of the below categories, first consider the need for an agency-specific provision, noting the above guidance on sharing activities which may already be permitted.

Table 2: Approach to information sharing categories

Category	Meaning
Category 1: General permission to share	Reflects a presumption in favour of sharing. A suitable default position which can be adopted in low to medium-risk environments, where sharing will support business, community and regulator efficiencies.
Category 2: Permission to share with limited restrictions	Reflects a presumption in favour of sharing, suitable for application to medium-risk environments where a regulator determines specific circumstances in which sharing should be restricted.
Category 3: Permission to share with substantial restrictions	This category should be avoided where possible as it can present unclear parameters. This is because extensive lists of restrictions may create significant legislative barriers to sharing. This approach may also contribute to a culture of reluctance to share across government. Consider whether Category 2 or 4 is more appropriate in regard to a presumption in favour of sharing.
Category 4: Obligation of confidentiality with limited permissions to share	Recognises that some high to medium-risk environments may warrant a confidentiality obligation but provides for sharing in some limited circumstances. Suitable for restricting disclosure of sensitive information (and should be used, where possible, in combination with a category 1 provision). Note that 'sensitive information' is defined in the <i>Privacy and Data Protection Act 2014</i> and there are obligations around the handling of sensitive information (see IPP 10).
Category 5: General obligation of confidentiality	Recognises that some high-risk, sensitive circumstances may warrant a general obligation of confidentiality.

Note: These categories consider (and are broadly consistent with) the OVIC's Business Impact Levels (BILs) which can be found here. Consideration of the BILs should form part of a holistic determination of the appropriate category, taking into account the questions below and the broader benefits of information sharing (or the risks of not sharing information).

Applying multiple categories

To respond appropriately to information sharing risks, a single regulatory scheme may introduce model provisions which reflect more than one of the identified categories, e.g. a scheme may generally employ a Category 1 approach but introduce a Category 5 provision for discrete and justifiable components.

Before implementing a model provision, policymakers should ask the following questions:

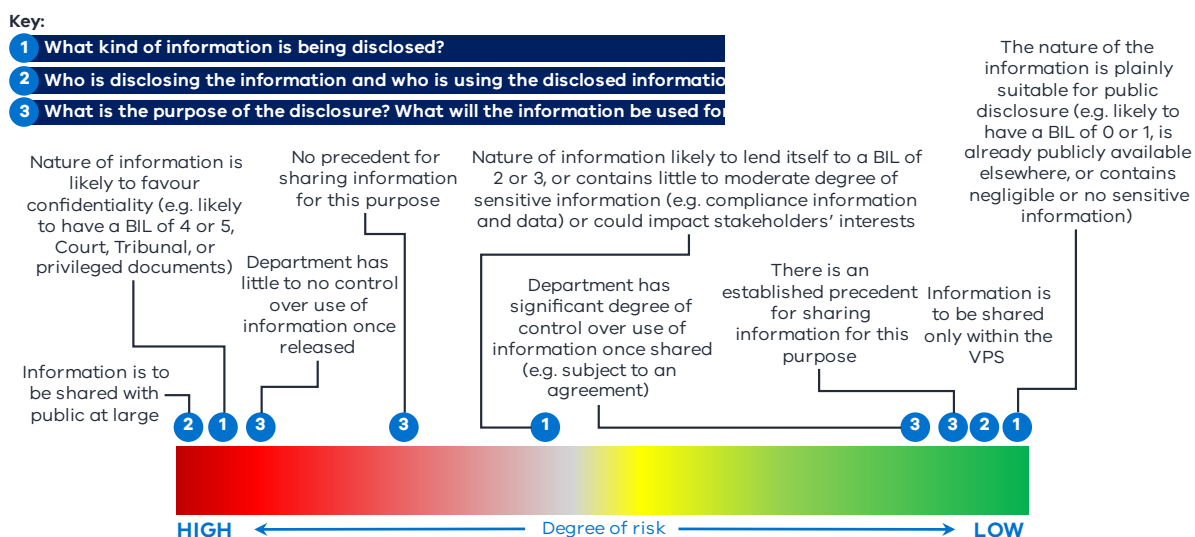
- **What kind of information being disclosed and/or used (e.g. personal information, health information, information captured by the *Data Sharing Act 2017* etc.)?**
- **Who is disclosing the information and who is using the disclosed information?**
- **What is the purpose of the disclosure? What will the information be used for?**

The risk associated with sharing (disclosing and/or receiving) information will differ depending on the answers to these questions. For example, there may be a lower level of risk associated with sharing information between Victorian government organisations, compared to sharing information with external organisations. External organisations may, for example, include individuals, regulated entities, regulators/law enforcement agencies in other jurisdictions, and the public.

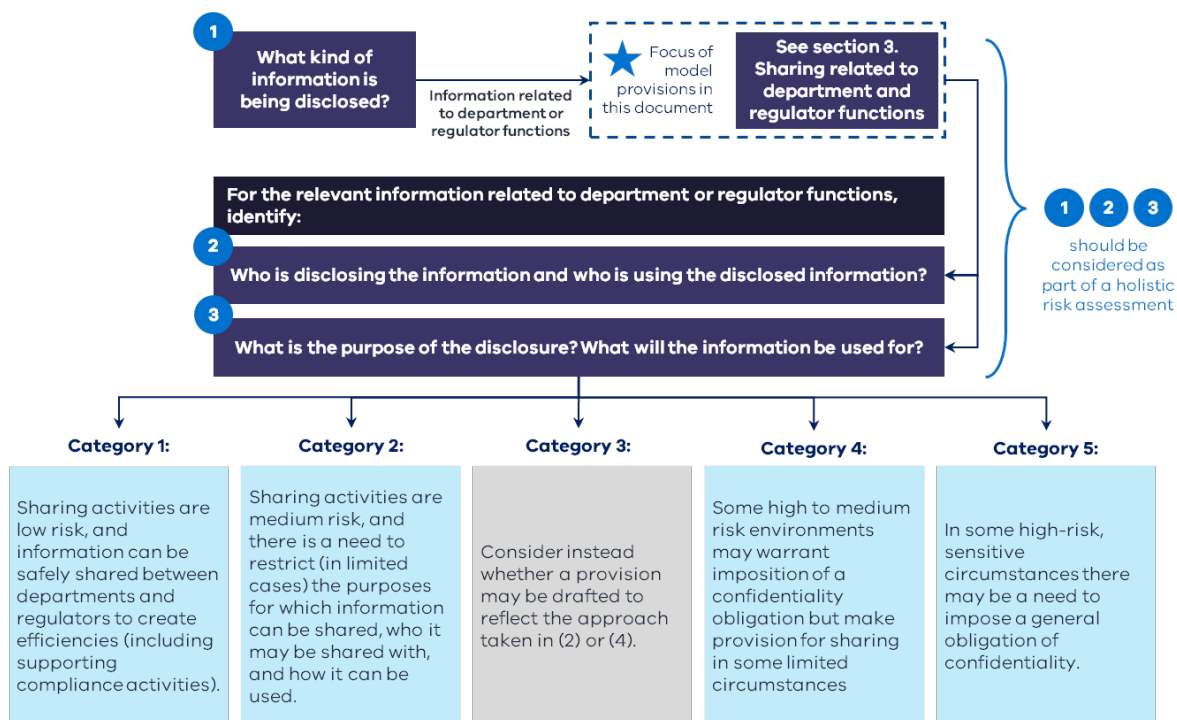
The diagram below sets out some potential factors which would likely impact the degree of risk associated with information sharing activities. It provides an indicative consideration of how the BILs might be considered within the context of the three key questions, providing a holistic response to help determine the appropriate category for legislative provisions.

Policymakers should identify the factors that are relevant to their risk assessments, consider them holistically, and develop an average risk rating for the information sharing activity that a provision may allow or constrain.

The diagram below shows the process policymakers should follow when conducting a risk assessment to determine the appropriate risk level category for the relevant regulatory environment.



In determining the applicable level of risk, policymakers should consider not only the risks associated with sharing information but also the risks and lost opportunities that may result from not sharing. For example, a limited ability to effectively regulate, address misconduct, or minimise disruptions to businesses and the community may justify moving an activity from Category 3 to Category 2, particularly if operational mitigations are in place. There should generally be a presumption in favour of allowing information sharing where appropriate, as this fosters a culture of collaboration and maximises the benefits of shared information.



Fostering an information sharing culture

Regardless of what legislative settings apply, an agency may be reluctant to share information if it does not have a positive information sharing culture.

An information sharing culture means there is openness to sharing information in appropriate circumstances and there are avenues in place to facilitate that sharing.

OVIC's guidance on fostering an information sharing culture

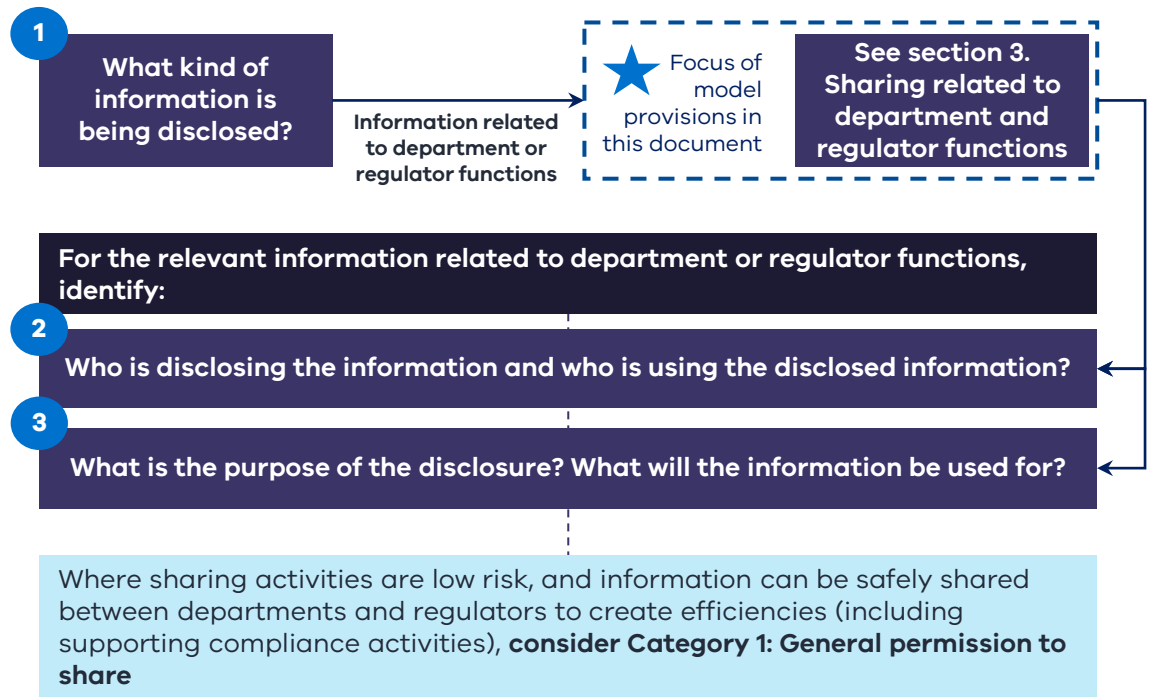
OVIC provides useful guidance on the pillars for fostering an information sharing culture:

- **Governance and accountability:** There should be a clear framework for information sharing activities which specifies roles, responsibilities and processes (all of which are aligned with applicable legislation). This may also include policy documents which set out how information should be shared in certain circumstances, and the factors which should be considered when deciding whether or not to share.
- **Transparency:** Organisations should be transparent about how they will handle information. This includes specifying the types of information which are collected, and how the information will be managed (including from a security and privacy perspective).
- **Training and awareness:** Employees should be aware of how to manage information in accordance with applicable legislation and the organisation's policies. Training should cover risk management processes which underpin sharing activities – including responsible decision-makers and the authorising processes to be undertaken before sharing.

OVIC's guidance can be accessed on [OVIC's website](#).

The sections below provide more detail on each category of information sharing.

3.1 Category 1: General permission to share



To support information sharing in low-risk environments, an agency's enabling legislation may contain general information sharing provisions. These provisions will set out purposes for which information can be shared, the kinds of information which can be shared and to whom information can be shared.

The purposes for sharing can include those linked to a person's functions or powers under the Act but may also be for other specified circumstances or purposes, such as promoting better inter-agency coordination, or assisting with general reporting by another agency.

Legislation may also allow for the creation of information sharing agreements (see the section below titled 'Information sharing agreements' for more guidance).

Policymakers should be aware of existing definitions and consider whether they are meaningful to adopt in their context.

Permission to use or disclose information

[*Policymakers should select the most appropriate option]

General permission to use or disclose information

Health information means—

Personal information means—

[**Note:** terms are to be defined meaningfully as is relevant to the context. Policymakers should be aware of the definitions of **personal information** and **health information** in the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001* respectively].

1.1 Permission to use information

A person engaged or employed by the [regulator] may use any information, including personal information and health information, obtained or held by the [regulator] under this Act if that use is necessary—

- * for that person to perform the person's functions or exercise the person's powers under this Act.
- * in [specified circumstances].
- * for [a specified purpose].

1.2 Permission to disclose information

A person engaged or employed by the [regulator] may disclose any information, including personal information and health information, obtained or held by the [regulator] under this Act to another person if that disclosure is necessary—

- * for the person disclosing the information to—
 - * perform their functions or exercise the powers under this Act [or any other Act].
 - * perform [a particular/specified function or exercise a particular/specified power].
- * for the other person to—
 - * perform the other person’s functions or exercise the other person’s powers under this Act [or Any other Act].
 - * perform [a particular/specified function or exercise a particular/specified power].
- * in [specified circumstances].
- * for [a specified purpose].

Example in practice – context for examples used throughout

Example details: *The Hammer Licensing Authority ('the Authority') is a statutory body established by the Hammers Act 2020. Its functions are licensing individuals to use hammers and monitoring of those licence-holders.*

The Hardware Health and Safety Act 2018 provides for health and safety of hardware users and regulation of hardware products. The Secretary to the Department of Hardware ('the Secretary') has functions and powers under the Act including approving hammers and monitoring hazardous hardware incidents. The Authority has advisory functions under this Act in relation to hammer approvals.

Example in practice

Health information has the same meaning as it has in section 3 of the Health Records Act 2001;

Personal information has the same meaning as it has in section 3 of the Privacy and Data Protection Act 2014;

1.1 Permission to use information

Example 1 – overview: permission to use information for functions and powers under an Act, assuming there is no other authority to use it (implied or otherwise):

A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary for that person to perform the person's functions or exercise the person's powers under the *Hardware Health and Safety Act 2018*.

Example 2 – overview: As at example 1, with the addition of prescribed person or class:

- (1) A person specified in subsection (2) may use any information, including personal information and health information, obtained or held by the person under this Act if that use is necessary for that specified person to perform the person's functions or exercise the person's powers under the *Hardware Health and Safety Act 2018*.
- (2) For the purposes of subsection (1), the following persons are specified—
 - (a) a person employed or engaged by the Authority; or
 - (b) a prescribed person or a person belonging to a prescribed class of person.

Example 3 – overview: permission to use information in specified circumstances:

A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary to prevent a risk of harm to any holder of a hammer licence.

Example 4 – overview: permission to use information for a specified purpose:

A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary for the Authority to advise the Secretary regarding the approval of a hammer under the *Hardware Health and Safety Act 2018*.

1.2 Permission to disclose information

Example 1 – overview: permission to disclose information for the person disclosing the information to perform their functions or exercise their powers under an Act:

A person employed or engaged by the Authority may disclose any information, including personal information and health information, obtained or held by the Authority under this Act to another person if that disclosure is necessary for the person disclosing the information to perform their functions or exercise their powers under this Act.

Example 2 – overview: permission to disclose information for the person disclosing the information to perform a specified function or exercise a specified power under an Act:

A person employed or engaged by the Authority may disclose any information, including personal information and health information, obtained or held by the Authority under this Act to another person if that disclosure is necessary for the person disclosing the information to determine whether to revoke a hammer licence under this Act.

Example 3 – overview: permission to disclose information to another person, for purposes of the other person performing their functions and powers under an Act:

A person employed or engaged by the Authority may disclose to the Secretary any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the Secretary to perform functions or exercise powers under the *Hardware Health and Safety Act 2018*.

Example 4 – overview: permission to disclose information to another person, for purposes of the other person performing specified functions or exercising specified powers under an Act:

A person employed or engaged by the Authority may disclose to the Secretary any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the Secretary to determine whether to approve a hammer under the *Hardware Health and Safety Act 2018*.

Information sharing agreements

What is an information sharing agreement?

Legislation may allow an information sharing agreement to be created between certain parties. These provisions offer a mechanism for parties to exchange information while performing their functions.

Information sharing agreements are recommended as best practice for categories 2 and 4 as they help establish clear operational expectations between entities. However, they do not always require an empowering legislative provision.

Before requesting provision for an information sharing agreement in legislation, policymakers should consider:

- whether the contemplated sharing activities may already be permitted (with reference to the considerations outlined on page 20), and
- if already permitted, the need for an information sharing agreement.

If the proposed sharing is already permitted under general laws, a specific provision to do so may add complexity or unduly restrict future flexibility.

Where there is desire (and an identified need) to create provisions for an information sharing agreement, policymakers should identify:

- who can be a party to an information sharing agreement
- the information that may be covered by an agreement
- the purposes for which information may be shared under an agreement
- any conditions which must be included in an agreement.

More specifically, policymakers should consider the specific uses and disclosures to be permitted under an agreement (and the rationale for these). Before engaging with OCPC, policymakers should prepare answers to the following questions:

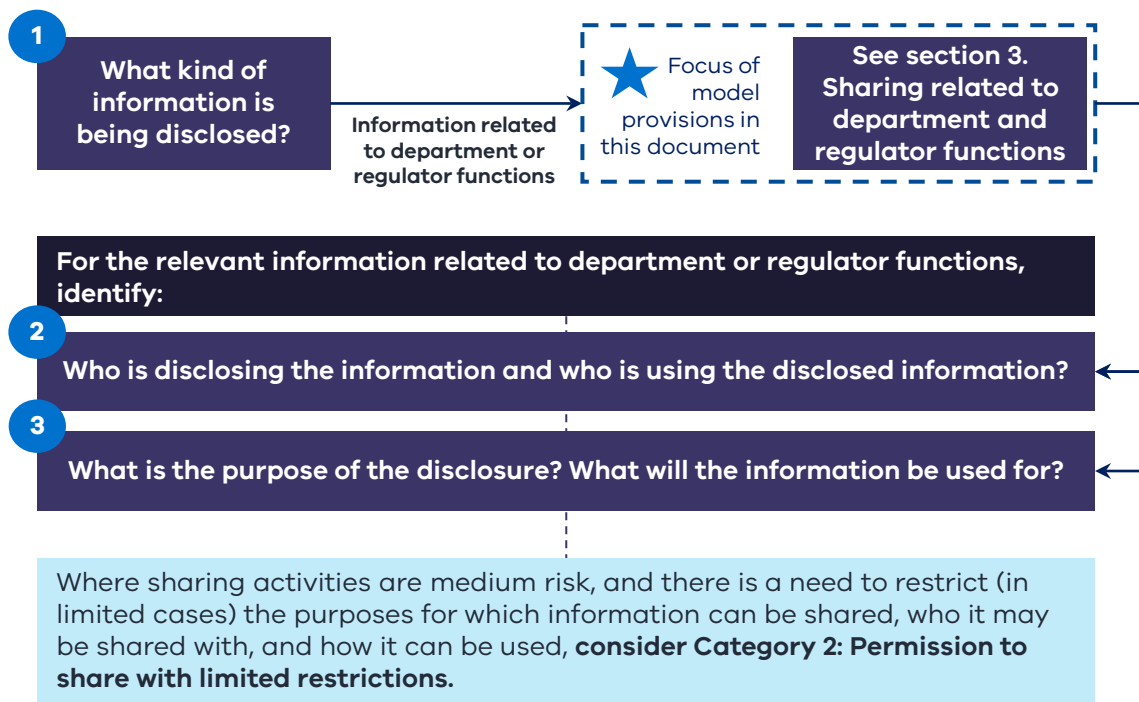
1. **What particular disclosure** is to be authorised by the information sharing agreement? Does this disclosure differ for Category 1 and for Category 2 (as defined in this guidance document)?
2. **What particular use** is to be authorised by the information sharing agreement? Does this use differ for Category 1 and for Category 2 (as defined in this guidance document)?
3. **For what purpose** is the information sharing agreement authorising the use or disclosure? For example, does the policymaker intend that disclosure or use in accordance with the agreement will be an authorisation under law for the purpose of other statutory exceptions?

Example

Section 259AB of the *Building Act 1993* allows the Victorian Building Authority to enter into an information sharing agreement with at least one other building regulator, as well as allowing sharing between other specified agencies (e.g. Consumer Affairs Victoria, the Architects Registration Board of Victoria, Cladding Safety Victoria, WorkCover, Victorian Managed Insurance Company and the Business Licensing Regulator).

The information shared must be reasonably necessary to assist in the performance of the Authority's functions or the functions of the relevant agency, party to the agreement, who is requesting information.

3.2 Category 2: Permission to share with limited restrictions



In medium-risk environments, there may be a need to limit the kinds of information, purposes, persons or entities which may be involved in information sharing. In these cases, there is a need to balance:

- an approach which favours sharing
- appropriate restrictions to manage risk.

The purposes for sharing can include purposes linked to a person's functions or powers under the Act but may also be for other specified circumstances or purposes, such as assisting other agencies with enforcement under their Acts.

Appropriate restrictions on sharing

Policymakers should consider and identify specific circumstances where there may be a need to restrict a general presumption in favour of sharing.

This may include, for example, a regime which supports a presumption in favour of sharing but restricts sharing in one of the following circumstances:

- The sharing of specific categories of information (such as personal information, health information or other sensitive information, such as commercially sensitive business information) or creating a category of ‘excluded information’
- The persons, classes of persons or entities to which information can be shared
- The persons, classes of persons or entities who can use information once shared, or

The sharing of information collected under specified sections in a particular Act.



Proportionality in practice

While there may be sound reasons to restrict information sharing, policymakers should prioritise an approach which favours sharing to the extent possible. This includes ensuring that any restrictions are proportionate to the risk that a policymaker is seeking to mitigate.

[Policymakers should select the most appropriate option*]

Use and disclosure with limited restrictions

Health information means—

Personal information means—

[**Note:** terms are to be defined meaningfully as is relevant to the context, noting there should be clear rationales for departing from existing definitions for these terms (see ‘Example in practice’ below)].

2.1 Exception to permission to use information [information limited]

(1) A person engaged or employed by the [regulator] may use any information, including personal information and health information, obtained or held by the [regulator] under this Act if that use is necessary—

- * for that person to perform the person’s functions or exercise the person’s powers under this Act.
- * in [specified circumstances].
- * for [a specified purpose].

(2) Subsection (1) does not apply in respect of—

- * any information obtained by or given to [regulator] under [relevant legislation].
- * any prescribed information or prescribed classes of information.
- * any **excluded information**. [**Note:** term is to be defined meaningfully as is relevant to the context].

2.2 Exception to permission to disclose information [information limited]

(1) A person engaged or employed by the [regulator] may disclose any information, including personal information and health information, obtained or held by the [regulator] under this Act to another person if that disclosure is necessary—

- * for the person disclosing the information to—
 - * perform their functions or exercise their powers under this Act [or any other Act].
 - * perform [a particular/specified function or exercise a particular/specified power].
- * for the other person to—
 - * perform the other person's functions or exercise the other person's powers under this Act [or any other Act].
 - * perform [a particular/specified function or exercise a particular/specified power].
- * in [specified circumstances].
- * for [a specified purpose].

(2) Subsection (1) does not apply in respect of—

- * any information obtained by or given to [regulator] under [relevant legislation].
- * any prescribed information or prescribed classes of information.
- * any **excluded information**. [**Note:** term is to be defined meaningfully as is relevant to the context].

Example in practice

Health information has the same meaning as it has in section 3 of the Health Records Act 2001;

Personal information has the same meaning as it has in section 3 of the Privacy and Data Protection Act 2014;

2.1 Exception to permission to use information [information limited]

Example 1 – overview: permission to use information for the person's functions and powers under an Act, subject to exception for information provided under specified legislation:

- (1) A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary for that person to perform the person's functions or exercise the person's powers under this Act.
- (2) Subsection (1) does not apply in respect of any information given to the Authority by the Secretary under Part 6 of the Hardware Health and Safety Act 2018.

Example 2 – overview: A permission to use information (other than excluded information) in specified circumstances:

Excluded information means—

- (a) information given to the Authority by the Secretary under Part 6 of the *Hardware Health and Safety Act 2018*; or
 - (b) prescribed information.
- (1) A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority if that use is necessary to prevent a risk of harm to any holder of a hammer licence.
- (2) Subsection (1) does not apply in respect of any information that is excluded information.

2.2 Exception to permission to disclose information [information limited]

Example 1 – overview: permission to disclose information to another person for that other person to perform specified functions or exercise specified powers, subject to an exception for prescribed information:

- (1) A person employed or engaged by the Authority may disclose to the Secretary any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the Secretary to determine whether to approve a hammer under the *Hardware Health and Safety Act 2018*.
- (2) Subsection (1) does not apply in respect of any prescribed information or prescribed class of information.

Example 2 – overview: permission to disclose information for a specified purpose subject to more than one exception:

- (1) A person employed or engaged by the Authority may disclose to another person any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the person disclosing the information to determine whether to grant a hammer licence to a person.
- (2) Subsection (1) does not apply in respect of—
- (a) any information given to the Authority by a law enforcement agency; or
 - (b) any prescribed information or prescribed class of information.

Limiting provisions on information sharing agreements

Information sharing agreements are recommended as best practice for Categories 2 and 4, but policymakers should consider whether regulators need their own specific provision or can rely on general laws.

Policymakers should engage directly with OCPC to develop provisions for an information sharing agreement, having first considered the questions on page 20.

Example

Section 60E of the *Essential Services Commission Act 2001* allows the Commission to enter into or approve an information sharing agreement with a number of specified and prescribed entities, including a fair trading agency, an essential services regulator or a law enforcement agency.

The information which can be shared under an agreement **is limited to specific types of information** (including information obtained under section 37, information concerning investigations, law enforcement, or information affecting the interests of consumers).

There are further limitations, including prohibitions on sharing specified information and limitations regarding confidential information.

Example in practice

3.1 Information sharing agreements [where purposes are specified]

Example 2 – overview: p information sharing agreement setting out information to which it relates and purpose for which the agreement may be used (Category 2)

- (1) The Authority may enter into an information sharing agreement with the Chainsaw Licensing Board that provides for—
 - (a) the Authority to disclose information held by the Authority and specified in the agreement to the Chainsaw Licensing Board; and
 - (b) the Chainsaw Licensing Board to disclose information held by the Board and specified in the agreement to the Authority.
- (2) An information sharing agreement provide for disclosure of any of the following information—
 - (a) information relating to monitoring of holders of licences under the *Chainsaws Act 2018* or the *Hammers Act 2020*;
 - (b) information affecting the interests of hardware users;
 - (c) prescribed information.
- (3) The Authority may use information disclosed under the information sharing agreement for the purposes of the Authority assessing licence applications under the *Hammers Act 2020*.
- (4) The Board may use information disclosed under the information sharing agreement for the purposes of the Board assessing licence applications under the *Chainsaws Act 2018*.

3.3 Category 3: Permission to share with substantial restrictions

No model provisions for Category 3

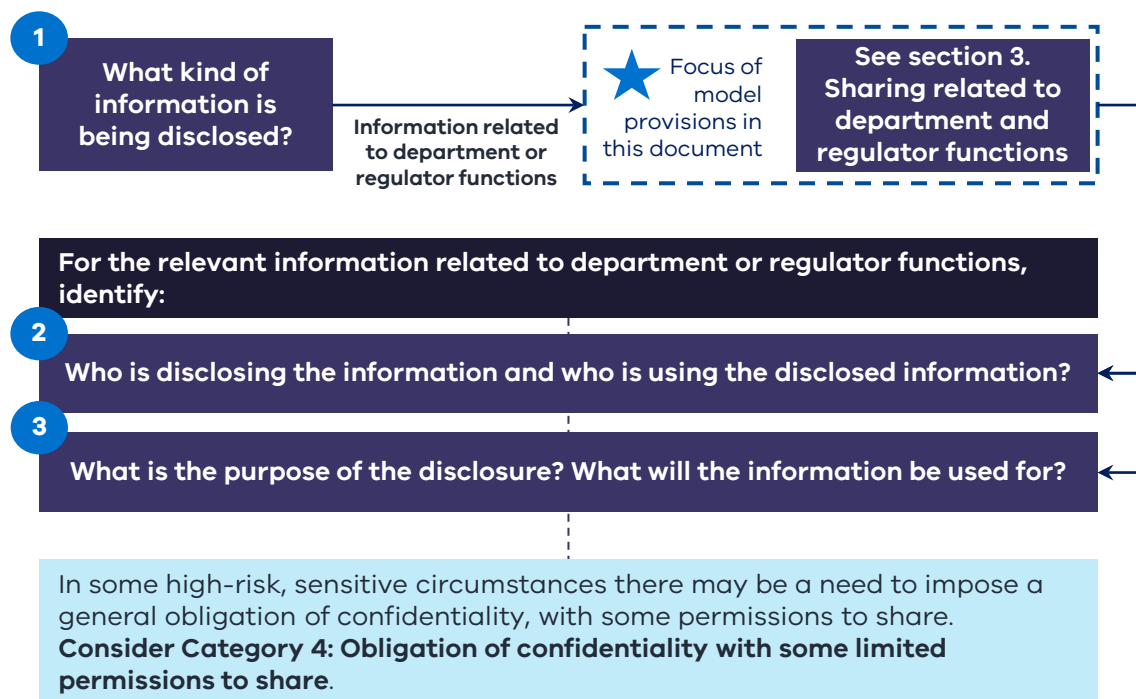
This document does not contain model provisions which reflect a Category 3 provision. This is because extensive lists of restrictions may create significant legislative barriers to sharing. This approach may also contribute to a culture of reluctance to share across government.

When a department identifies that a Category 3 provision may be appropriate, or where a Category 3 provision already exists in a department's enabling legislation, policymakers should consider whether:

- the extensive list of restrictions is justified, given impact on the presumption in favour of sharing
- a provision may instead be crafted to adopt the approach taken in (2), by reducing the number of restrictions applied to sharing activities
- a provision may instead be crafted to adopt the approach taken in (4), where there is a justified need for a presumption of confidentiality with some limited opportunities for sharing.

Policymakers who are contemplating Category 3 may wish to consider a mixed approach (for example, Category 2 for most elements of the proposed sharing activities and Category 4 only for elements that are higher risk).

3.4 Category 4: Obligation of confidentiality with some limited permissions to share



Some high-to-medium risk environments warrant the inclusion of a confidentiality obligation. This may include, for example, where sharing of the information:

- may create a risk to life, health or safety
- may prejudice an investigation or ongoing legal proceeding
- may create a threat to national safety or security.

However, even where there is a baseline need for a confidentiality provision, **sharing may be appropriate in some limited circumstances**, e.g. sharing:

- with the explicit consent of the person to whom the information relates, or is communicated by the person to whom the information relates
- with an integrity agency or in the course of specific court or tribunal proceedings
- to prevent harm to an individual's life, health or wellbeing
- to prevent harm to the health, safety or welfare of the public.

Where an agency has an exemption under the *Spent Convictions Act 2021*, the relevant category of permitted information sharing is likely to be Category 4 as there are only limited circumstances in which a regulator can share spent conviction information – see section 22(3) of that Act. The relevant legislation should identify which spent convictions can be considered by a regulator so that only convictions relevant to their function are considered.

Confidentiality obligations may also be applied to certain groups of people (rather than ‘any person’) to limit the restrictiveness of the provision. This could include, for example, application to:

- government employees or persons otherwise engaged by government to perform a specific function or activity
- current and former government employees
- a specific professional or occupational group
- Ministers or parliamentary officers
- those working within a court or tribunal.

Provisions may also apply to identified conduct, such as copying or recording, rather than information sharing at large.

Example

Section 57(1) of the *Disability Service Safeguards Act 2018* creates a duty of confidentiality for persons in relation to information obtained during the course of a conciliation.

However, section 57(2) allows disclosure of information in some circumstances including where there is a belief on reasonable grounds that the disclosure is necessary to avoid a serious risk to a person’s life, health, safety or welfare, or the public’s health, safety or welfare.

Section 57(2)(b) also permits disclosure where the disclosure is made with the written agreement of the person to whom the information relates.

[Policymakers should select the most appropriate option*]

Obligation of confidentiality

4.1 Offence to disclose information

(1) A person engaged or employed by the [regulator] must not disclose information acquired by the [regulator] in performing a function or exercising a power under [relevant information]—

- * other than in the circumstances specified in subsection (2).
- * unless the disclosure is permitted under subsection (2).

Penalty:

(2) For the purposes of subsection (1), the circumstances are that the disclosure is—

- (a) required, authorised or permitted by or under this Act or any other Act; or
- (b) with the express consent of the person to whom it relates; or
- (c) to [an integrity agency]; or
- (d) to a court or tribunal in the course of any legal proceeding or pursuant to an order of a court or tribunal; or
- (e) to prevent harm to the life, health or wellbeing of an individual; or
- (f) to prevent harm to the health, safety or welfare of the public.

Example in practice

4.1 Offence to disclose information

Example 1 – overview: offence to disclose information acquired in performing functions or exercising powers under specified legislation unless permitted:

- (1) A person employed or engaged by the Authority must not disclose information acquired by the person in performing a function or exercising a power under this Act or the *Hardware Health and Safety Act 2020* unless the disclosure is permitted under subsection (2).

Penalty:

- (2) For the purposes of subsection (1), the disclosure of the information is permitted if it is—
 - (a) required, authorised or permitted by or under this Act or any other Act; or
 - (b) with the express consent of the person to whom it relates; or
 - (c) to [an integrity agency]; or
 - (d) to a court or tribunal in the course of any legal proceeding or pursuant to an order of a court or tribunal; or
 - (e) to prevent harm to the life, health or wellbeing of an individual; or
 - (f) to prevent harm to the health, safety or welfare of the public.

Example 2 – overview: offence to disclose information acquired in performing functions or exercising powers under specified legislation other than in specified circumstances:

- (1) A person employed or engaged by the Authority must not disclose information acquired by the person in performing a function or exercising a power under this Act or the *Hardware Health and Safety Act 2020* other than in circumstances specified in subsection (2).

Penalty:

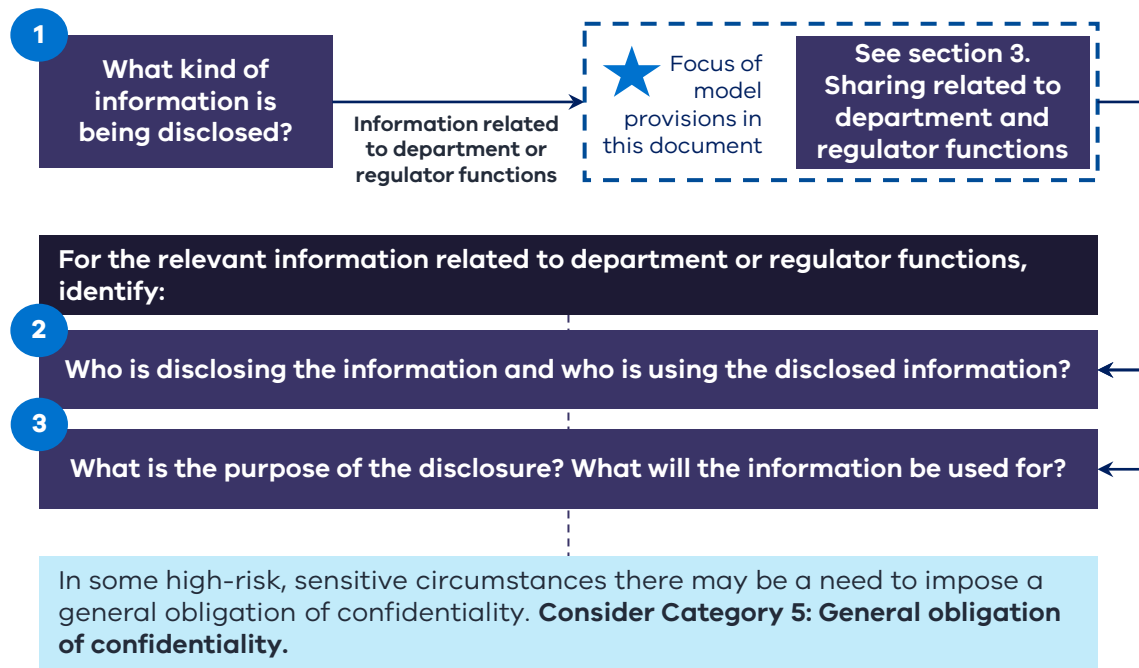
- (2) For the purposes of subsection (1), the circumstances are that the disclosure is—
 - (a) required, authorised or permitted by or under this Act or any other Act; or
 - (b) with the express consent of the person to whom it relates; or
 - (c) to [an integrity agency]; or
 - (d) to a court or tribunal in the course of any legal proceeding or pursuant to an order of a court or tribunal; or
 - (e) to prevent harm to the life, health or wellbeing of an individual; or
 - (f) to prevent harm to the health, safety or welfare of the public.

Example 3 – overview: offence to disclose information acquired in performing functions or exercising powers under specified legislation:

A person employed or engaged by the Authority must not disclose information acquired by the person in performing a function or exercising a power under this Act or the *Hardware Health and Safety Act 2020* unless the disclosure is permitted under subsection (2).

Penalty:

Policymakers should engage directly with the OVIC, any relevant departments, instructors, and OCPC on the nature of confidentiality. Policymakers should engage with OCPC and the Department of Justice and Community Safety (email CCLConsultation@justice.vic.gov.au) on any appropriate offence provisions or other penalties for specific legislation.



3.5 Category 5: General obligation of confidentiality

Confidentiality provisions are appropriate only for particularly high-risk, sensitive circumstances, including:

- government-related information, which may not be in the public interest to share
- information which, if shared, may be inherently harmful to an individual's life, health or welfare
- information which, if shared, may compromise court or other legal proceedings.



Proportionality in practice

Confidentiality provisions are very restrictive by nature. Policymakers should ensure that the inclusion of a confidentiality provision can be justified and is proportionate to the risk or identified harm which policymakers are seeking to mitigate.

The model provision set out above at section 3.4 provides a starting point for policymakers to formulate a provision in favour of confidentiality appropriate for a Category 5 risk environment. However, such confidentiality provisions should be specific to the regulatory environment, including the risks a policymaker is seeking to mitigate. Policymakers should engage directly with OCPC to ensure the provisions appropriately reflect the regulatory context.

Policymakers should note that the *Victorian Data Sharing Act 2017* allows data to be shared with the Chief Data Officer', even if a secrecy provision would otherwise prevent this if it is in accordance with, and for the purposes of, the *Victorian Data Sharing Act 2017* (see Division 2 of Part 4).

Offences for unlawful disclosure

Unlawful disclosure of information or contravention of an applicable secrecy provision may attract a criminal penalty. Policymakers should engage directly with OCPC to develop these provisions, to ensure they are fit for purpose.

Policymakers should also engage directly with OVIC, other relevant departments, instructors, and OCPC on the nature of confidentiality. Policymakers should engage with OCPC and the Department of Justice and Community Safety (email CCLConsultation@justice.vic.gov.au) on any appropriate offence provisions or other penalties for specific legislation.

Appendix A – Consolidated Model Provisions provided by OCPC

Model provisions	Example
<p>[*select appropriate option]</p>	<p><i>Example details:</i></p> <p><i>The Hammer Licensing Authority ('the Authority') is a statutory body established by the Hammers Act 2020. Its functions are licensing individuals to use hammers and monitoring of those licence holders.</i></p> <p><i>The Hardware Health and Safety Act 2018 provides for health and safety of hardware users and regulation of hardware products. The Secretary to the Department of Hardware ('the Secretary') has functions and powers under the Act including approving hammers and monitoring hazardous hardware incidents. The Authority has advisory functions under this Act in relation to hammer approvals.</i></p>
<p>Category 1—general permission to use or disclose information</p>	
<p><i>health information</i> means— <i>personal information</i> means— <i>Note: to be defined meaningfully as is relevant to the context. Policymakers should be aware of the definitions of personal information and health information in the Privacy and Data Protection Act 2014 and the Health Records Act 2001 respectively.</i></p> <p>1.1 Permission to use information</p> <p>A person engaged or employed by the [regulator] may use any information, including personal information and health information, obtained or held by the [regulator] under this Act if that use is necessary—</p> <p>*for that person to perform the person's functions or exercise the person's powers under this Act.</p> <p>*in [specified circumstances].</p> <p>*for [a specified purpose].</p>	<p><i>health information has the same meaning as it has in section 3 of the Health Records Act 2001;</i></p> <p><i>personal information has the same meaning as it has in section 3 of the Privacy and Data Protection Act 2014;</i></p> <p>1.1 Permission to use information</p> <p><i>Example 1: permission to use information for functions and powers under an Act, assuming there is no other authority to use it (implied or otherwise):</i></p> <p>A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary for that person to perform the person's functions or exercise the person's powers under the Hardware Health and Safety Act 2018.</p>

Model provisions	Example
<p>1.2 Permission to disclose information</p> <p>A person engaged or employed by the [regulator] may disclose any information, including personal information and health information, obtained or held by the [regulator] under this Act to another person if that disclosure is necessary—</p> <p>*for the person disclosing the information to—</p> <ul style="list-style-type: none"> *perform their functions or exercise their powers under this Act [or any other Act]. *perform [a particular/specified function or exercise a particular/specified power]. 	<p><i>Example 2: As at example 1, with the addition of prescribed person or class</i></p> <ol style="list-style-type: none"> (1) A person specified in subsection may use any information, including personal information and health information, obtained or held by the person under this Act if that use is necessary for that specified person to perform the person’s functions or exercise the person’s powers under the Hardware Health and Safety Act 2018. (2) For the purposes of subsection (1), the following persons are specified— <ol style="list-style-type: none"> (a) a person employed or engaged by the Authority; or (b) a prescribed person or a person belonging to a prescribed class of person. <p><i>Example 3: permission to use information in specified circumstances</i></p> <p>A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary to prevent a risk of harm to any holder of a hammer licence.</p> <p><i>Example 4: permission to use information for a specified purpose</i></p> <p>A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary for the Authority to advise the Secretary regarding the approval of a hammer under the Hardware Health and Safety Act 2018.</p> <p>1.2 Permission to disclose information</p> <p><i>Example 1: permission to disclose information for the person disclosing the information to perform their functions or exercise their powers under an Act</i></p> <p>A person employed or engaged by the Authority may disclose any information, including personal information and health information, obtained or held by the Authority under this Act to another person if that disclosure is necessary for the person disclosing the information to perform their functions or exercise their powers under this Act.</p>

Model provisions	Example
<p>*for the other person to—</p> <ul style="list-style-type: none"> *perform the other person’s functions or exercise the other person’s powers under this Act [or any other Act]. *perform [a particular/specified function or exercise a particular/specified power]. <p>*in [specified circumstances].</p>	<p><i>Example 2: permission to disclose information for the person disclosing the information to perform a specified function or exercise a specified power under an Act</i></p> <p>A person employed or engaged by the Authority may disclose any information, including personal information and health information, obtained or held by the Authority under this Act to another person if that disclosure is necessary for the person disclosing the information to determine whether to revoke a hammer licence under this Act.</p> <p><i>Example 3: permission to disclose information to another person, for purposes of the other person performing their functions and powers under an Act</i></p> <p>A person employed or engaged by the Authority may disclose to the Secretary any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the Secretary to perform functions or exercise powers under the Hardware Health and Safety Act 2018.</p> <p><i>Example 4: permission to disclose information to another person, for purposes of the other person performing specified functions or exercising specified powers under an Act</i></p> <p>A person employed or engaged by the Authority may disclose to the Secretary any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the Secretary to determine whether to approve a hammer under the Hardware Health and Safety Act 2018.</p>
<p>Category 2—use and disclosure with limited restrictions</p>	
<p><i>health information</i> means—</p> <p><i>personal information</i> means—</p> <p><i>Note: to be defined meaningfully as is relevant to the context.</i></p> <p>2.1 Exception to permission to use information [information limited]</p>	<p><i>health information</i> has the same meaning as it has in section 3 of the Health Records Act 2001;</p> <p><i>personal information</i> has the same meaning as it has in section 3 of the Privacy and Data Protection Act 2014;</p> <p>2.1 Exception to permission to use information [information limited]</p> <p><i>Example 1: permission to use information for the person’s functions and powers under an Act, subject to exception for information provided under specified legislation</i></p>

Model provisions	Example
<p>(1) A person engaged or employed by the [regulator] may use any information, including personal information and health information, obtained or held by the [regulator] under this Act if that use is necessary—</p> <ul style="list-style-type: none"> *for that person to perform the person's functions or exercise the person's powers under this Act. *in [specified circumstances]. *for [a specified purpose]. <p>(2) Subsection (1) does not apply in respect of—</p> <ul style="list-style-type: none"> *any information obtained by or given to [regulator] under [relevant legislation]. *any prescribed information or prescribed class of information. *any <i>excluded information</i>. <p>2.2 Exception to permission to disclose information [information limited]</p> <p>(1) A person engaged or employed by the [regulator] may disclose any information, including personal information and health information, obtained or held by the [regulator] under this Act to another person if that disclosure is necessary—</p> <ul style="list-style-type: none"> *for the person disclosing the information to— <ul style="list-style-type: none"> *perform their functions or exercise their powers under this Act [or any other Act]. *perform [a particular/specified function or exercise a particular/specified power]. *for the other person to— <ul style="list-style-type: none"> *perform the other person's functions or exercise the other person's powers under this Act [or any other Act]. *perform [a particular/specified function or exercise a particular/specified power]. 	<p>(1) A person employed or engaged by the Authority may use any information, including personal information and health information, obtained or held by the Authority under this Act if that use is necessary for that person to perform the person's functions or exercise the person's powers under this Act.</p> <p>(2) Subsection (1) does not apply in respect of any information given to the Authority by the Secretary under Part 6 of the Hardware Health and Safety Act 2018.</p> <p><i>Example 2: permission to use information (other than excluded information) in specified circumstances</i></p> <p><i>excluded information</i> means—</p> <ul style="list-style-type: none"> (a) information given to the Authority by the Secretary under Part 6 of the Hardware Health and Safety Act 2018; (b) prescribed information. <p>(1) A person employed or engaged by the Authority may use any information, including personal information and health information, held by the Authority if that use is necessary to prevent a risk of harm to any holder of a hammer licence.</p> <p>(2) Subsection (1) does not apply in respect of any information that is excluded information.</p> <p>2.2 Exception to permission to disclose information [information limited]</p> <p><i>Example 1: permission to disclose information to another person for that other person to perform specified functions or exercise specified powers, subject to an exception for prescribed information</i></p> <p>(1) A person employed or engaged by the Authority may disclose to the Secretary any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the Secretary to determine whether to approve a hammer under the Hardware Health and Safety Act 2018.</p> <p>(2) Subsection (1) does not apply in respect of any prescribed information or prescribed class of information.</p>

Model provisions	Example
<p>*in [specified circumstances].</p> <p>*for [a specified purpose].</p> <p>(2) Subsection (1) does not apply in respect of—</p> <p>*any information obtained by or given to [regulator] under [relevant legislation].</p> <p>*any prescribed information or prescribed class of information.</p> <p>*any excluded information.</p>	<p><i>Example 2: permission to disclose information for a specified purpose subject to more than one exception</i></p> <p>(1) A person employed or engaged by the Authority may disclose to another person any information, including personal information and health information, obtained or held by the Authority under this Act if that disclosure is necessary for the person disclosing the information to determine whether to grant a hammer licence to a person.</p> <p>(2) Subsection (1) does not apply in respect of—</p> <p>(a) any information given to the Authority by a law enforcement agency; or</p> <p>(b) any prescribed information or prescribed class of information.</p>
<p>Category 4 and Category 5—Obligation of confidentiality</p>	
<p>3.1 Offence to disclose information</p> <p>(1) A person engaged or employed by the [regulator] must not disclose information acquired by the [regulator] in performing a function or exercising a power under [relevant legislation]—</p> <p>*other than in the circumstances specified in subsection (2).</p> <p>*unless the disclosure is permitted under subsection (2).</p> <p>Penalty:</p> <p>* (2) For the purposes of subsection (1), the circumstances are that the disclosure is—</p> <p>(a) required, authorised or permitted by or under this Act or any other Act; or</p> <p>(b) with the express consent of the person to whom it relates; or</p> <p>(b) to [an integrity agency]; or</p> <p>(c) to a court or tribunal in the course of any legal proceeding or pursuant to an order of a court or tribunal; or</p> <p>(d) to prevent harm to the life, health or wellbeing of an individual; or</p> <p>(e) to prevent harm to the health, safety or welfare of the public.</p>	<p>3.1 Offence to disclose information</p> <p><i>Example 1: offence to disclose information acquired in performing functions or exercising powers under specified legislation unless permitted</i></p> <p>(1) A person employed or engaged by the Authority must not disclose information acquired by the person in performing a function or exercising a power under this Act or the Hardware Health and Safety Act 2020 unless the disclosure is permitted under subsection (2).</p> <p>Penalty:</p> <p>(2) For the purposes of subsection (1), the disclosure of information is permitted if it is—</p> <p>(a) required, authorised or permitted by or under this Act or any other Act; or</p> <p>(b) with the express consent of the person to whom it relates; or</p> <p>(b) to [an integrity agency]; or</p> <p>(c) to a court or tribunal in the course of any legal proceeding or pursuant to an order of a court or tribunal; or</p> <p>(d) to prevent harm to the life, health or wellbeing of an individual; or</p> <p>(e) to prevent harm to the health, safety or welfare of the public.</p>

Model provisions	Example
	<p><i>Example 2: offence to disclose information acquired in performing functions or exercising powers under specified legislation other than in specified circumstances</i></p> <p>(1) A person employed or engaged by the Authority must not disclose information acquired by the person in performing a function or exercising a power under this Act or the Hardware Health and Safety Act 2020 other than in circumstances specified in subsection (2).</p> <p>Penalty:</p> <p>(2) For the purposes of subsection (1), the circumstances are that the disclosure is—</p> <ul style="list-style-type: none"> (a) required, authorised or permitted by or under this Act or any other Act; or (b) with the express consent of the person to whom it relates; or (b) to [an integrity agency]; or (c) to a court or tribunal in the course of any legal proceeding or pursuant to an order of a court or tribunal; or (d) to prevent harm to the life, health or wellbeing of an individual; or (e) to prevent harm to the health, safety or welfare of the public. <p>3.1 Offence to disclose information</p> <p><i>Example: offence to disclose information acquired in performing functions or exercising powers under specified legislation</i></p> <p>A person employed or engaged by the Authority must not disclose information acquired by the person in performing a function or exercising a power under this Act or the.</p> <p>Penalty:</p>

Model provisions	Example
<p>Categories 1 and 2—information sharing agreements</p>	
<p>4.1 Information sharing agreements</p> <p>(1) A [regulator] may enter into an information sharing agreement with [entity] that provides for—</p> <p style="padding-left: 20px;">*of any of the following information—</p> <p style="padding-left: 40px;">(a) [specify information].</p> <p style="padding-left: 20px;">* for any of the following purposes—</p> <p style="padding-left: 40px;">(a) [specify purpose].</p> <p>(2) An information sharing agreement may provide for disclosure—</p> <p>* (3) The [regulator/entity] may use information disclosed under the information sharing agreement—</p> <p style="padding-left: 20px;">*in the performance of the [regulator's/entity's] functions or exercise of the [regulator's/entity's] powers under this Act.</p> <p style="padding-left: 20px;">*for a purpose specified in the agreement.</p>	<p><i>Additional example details: under the Chainsaws Act 2018, the Chainsaw Licensing Board licences individuals to use chainsaws and monitors holders of those licences</i></p> <p>4.1 Information sharing agreements [purposes not specified]</p> <p><i>Example 1: information sharing agreement setting out information to which it relates (Category 1)</i></p> <p>(1) The Authority may enter into an information sharing agreement with the Chainsaw Licensing Board that provides for—</p> <p style="padding-left: 20px;">(a) the Authority to disclose information held by the Authority and specified in the agreement to the Chainsaw Licensing Board; and</p> <p style="padding-left: 20px;">(b) the Chainsaw Licensing Board to disclose information held by the Board and specified in the agreement to the Authority.</p> <p>(2) An information sharing agreement may provide for disclosure of any of the following information—</p> <p style="padding-left: 20px;">(a) information relating to monitoring of holders of licences under the Chainsaws Act 2018 or the Hammers Act 2020;</p> <p style="padding-left: 20px;">(b) information affecting the interests of hardware users;</p> <p style="padding-left: 20px;">(c) prescribed information.</p> <p>4.1 Information sharing agreements [purposes specified]</p> <p><i>Example 2: information sharing agreement setting out information to which it relates and purpose for which the agreement may be used (Category 2)</i></p> <p>(1) The Authority may enter into an information sharing agreement with the Chainsaw Licensing Board that provides for—</p> <p style="padding-left: 20px;">(a) the Authority to disclose information held by the Authority and specified in the agreement to the Chainsaw Licensing Board; and</p>

Model provisions	Example
	<p>(b) the Chainsaw Licensing Board to disclose information held by the Board and specified in the agreement to the Authority.</p> <p>(2) An information sharing agreement may provide for disclosure of any of the following information—</p> <ul style="list-style-type: none"> (a) information relating to monitoring of holders of licences under the Chainsaws Act 2018 or the Hammers Act 2020; (b) information affecting the interests of hardware users; (c) prescribed information. <p>(3) The Authority may use information disclosed under the information sharing agreement for the purposes of the Authority assessing licence applications under the Hammers Act 2020.</p> <p>(4) The Board may use information disclosed under the information sharing agreement for the purposes of the Board assessing licence applications under the Chainsaws Act 2018.</p>

Appendix B – Consolidated list of resources

Document title	URL (if applicable)
Better Regulation <i>Victoria's Towards best practice guide for regulators</i>	https://www.vic.gov.au/towards-best-practice-guide-regulators
Information about OVIC's Business Impact Levels (BILs)	https://ovic.vic.gov.au/information-security/victorian-protective-data-security-framework-business-impact-level-table-v2-1/
OIPC Legislative Process handbook	https://content.vic.gov.au/sites/default/files/2020-06/Legislative-Process-Handbook-June2020.pdf
Office of the Victorian Information Commissioner's (OVIC) guidance on information sharing and privacy	<ul style="list-style-type: none"> • https://ovic.vic.gov.au/privacy/resources-for-organisations/information-sharing-and-privacy/ • https://ovic.vic.gov.au/privacy/resources-for-organisations/information-sharing-and-privacy/#establishing-an-information-sharing-culture
OVIC flow chart on departmental decision-making	https://ovic.vic.gov.au/wp-content/uploads/2021/02/Information-sharing-flowchart.pdf
OVIC information about the PDPA and the operation of the IPPs	https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-pdp-act-a-deep-dive/
Service Victoria Identity Verification Standards	https://service.vic.gov.au/about-us/service-victoria-identity-verification-standards
Victorian Government's guidance on the Health Records Act	https://www.health.vic.gov.au/legislation/health-records-act
Victorian Government's guidance on the VDS Act	https://www.vic.gov.au/sites/default/files/2019-03/Victorian-Data-Sharing-Act-2017-web-guidance.pdf
Victorian Protective Data Security Framework	https://www.vic.gov.au/cyber-security-standards-and-guidelines

