Guidelines for sharing personal information
Issued March 2016
Guidelines for sharing personal information

Issued March 2016
Contents

Preface ............................................................................................................................... 6
Scope ................................................................................................................................. 7

Part 1: Introduction to information sharing ........................................................................ 8
What is information sharing? .............................................................................................. 8
Types of information sharing .............................................................................................. 9
Systematic information sharing ......................................................................................... 9
Ad hoc information sharing ............................................................................................... 9
Importance of responsible information sharing ............................................................... 10
Overview of the information sharing process .................................................................. 10

Part 2: Information sharing benefits and barriers ............................................................. 11
Benefits of information sharing ......................................................................................... 11
Benefits to the public .......................................................................................................... 11
Greater efficiency for organisations ................................................................................... 11
Confidence in data quality ................................................................................................ 11
Greater trust and confidence in government ................................................................. 11

Benefits to the public ......................................................................................................... 12
Convenience for citizens .................................................................................................... 12
Better integrated services .................................................................................................. 12
Enhanced protection for vulnerable people ....................................................................... 12

Constraints in enabling legislation ................................................................................... 12
Constraints in privacy law .................................................................................................. 13
Lack of leadership .............................................................................................................. 13

Cultural and institutional barriers .................................................................................... 13
Interoperability and compatibility issues ........................................................................... 14
Lack of trust ...................................................................................................................... 14
Fear of financial or reputational damage ........................................................................... 14

Part 3: Sharing personal information:
A methodology .............................................................................................................. 15

Before you decide to share .............................................................................................. 15
Step 1: Identify the type of personal information you are dealing with ......................... 15
Step 2: Understand your authorising environment ........................................................... 16
Legal authority to share .................................................................................................... 16
Confidentiality and secrecy ............................................................................................... 16
Privacy law ....................................................................................................................... 17
The Charter of Human Rights and Responsibilities ..................................................... 17
Consent ............................................................................................................................. 17

Step 3: Undertake a risk assessment .................................................................................. 18
 Necessary, proportionate, timely and secure ................................................................. 18
Interoperability and compatibility .................................................................................... 18
Privacy impact assessment ............................................................................................... 19
Risk in not sharing .......................................................................................................... 19

Step 4: Seek advice where necessary ............................................................................. 19
Legal advice ..................................................................................................................... 19
Advice from the Commissioner for Privacy and Data Protection .................................. 19
Preface

Information sharing is a concept that is a constant theme within the public sector, as one component of what is variously known as ‘joined-up government’, ‘networked government’, ‘horizontal government’, ‘whole of government’, ‘integrated government’, and ‘breaking down the silos’.

Information sharing is not a new phenomenon. It is generally traced to the election of the first Blair government in the UK in 1997. It emphasises the need for cross-government collaboration to:

• address public policy issues that extend beyond the remit of any one government agency
• promote efficiency and the better use of resources through improved coordination
• provide better services to the community.

Better information sharing – in many cases of personal information – is identified as underpinning these objectives. Although information sharing as a concept has a long history, the Victorian public sector has struggled to achieve effective and appropriate information sharing in practice.

The discussions that the Office of the Commissioner for Privacy and Data Protection (CPDP) has participated in across the Victorian public sector suggests widespread uncertainty about how to share personal information.

Privacy is often named as the primary impediment to information sharing – that is simply not the case. Privacy legislation – rather than preventing the sharing of personal information– places important limitations around the circumstances under which it can be shared, and with whom it can be shared. Instead, information sharing is often hampered by a general reluctance to disclose personal information due to misunderstandings of privacy law, confidentiality clauses, poor governance, interoperability issues and a persistent risk averse culture.

The phrase ‘information sharing’ cannot be found in Victorian legislation, although it is frequently referenced in policies, reports, and operational processes and procedures. The need for this guidance document stems from a wide-spread lack of understanding across government as to what personal information public sector organisations can or should share, when it is appropriate to share, and how decisions should be made about whether or not to share; what constitutes ‘information sharing’ can also at times be a subject of uncertainty.

Questions around the secondary use and disclosure of personal information have also proven to be a point of contention and uncertainty. Privacy laws are built on the fundamental principle that personal information collected for one purpose should not be used or disclosed for a secondary purpose. The experiences of privacy regulators demonstrate that in many cases there is an uneasiness about sharing personal information for a secondary purpose, even where permissible. Simultaneously, in cases where personal information is shared, practices are not always consistent with legal obligations and may expressly interfere with individuals’ information privacy rights.

Recognising the need for consolidated, authoritative guidance, this document has been produced to help improve understandings of information sharing across all levels of the Victorian public sector. The guidelines focus in particular on three key information management domains:

• information privacy
• protective data security
• recordkeeping.

By their very nature, the guidelines embody a Privacy by Design (PbD) philosophy to approaching information sharing activities, encouraging organisations to manage privacy before they enter into an information sharing arrangement. Although the guidelines are not legally binding, the steps and protective measures outlined are considered by CPDP to be best practice.
The purpose of these guidelines is to:

• identify the barriers faced when sharing personal information
• identify the questions that need to be asked when deciding whether or not to participate in information sharing initiatives
• set out the steps and processes necessary to address complex information sharing initiatives
• provide organisations with the tools required to ensure best practices in information sharing.

The document is divided into five main parts. Parts 1 and 2 provide the policy background and rationale for the guidelines, outlining what information sharing entails, why proper information sharing is important to the public sector, and what the current barriers to information sharing are that need to be overcome. Parts 3 to 5 provide practical guidance in relation to the principles and processes that need to be considered before information can be shared.

**Scope**

These guidelines have been developed for the Victorian public sector. By virtue of the outsourcing arrangements that are typical to delivering government services, some private sector organisations may also find this document useful in understanding their responsibilities when sharing information under state contract.

These guidelines are written to reflect information sharing practices that involve personal information\(^1\) – non-identifiable and de-identified information are expressly excluded from the scope of this guidance. Health information is also outside the scope of these guidelines. Those seeking advice on sharing health information are encouraged to contact the Office of the Health Services Commissioner.

The guidelines focus heavily on ensuring that information sharing is conducted in ways that are consistent with information privacy and data security. Although the right to privacy and security of information are extremely important, they do not always outweigh other interests. The right to life and safety for instance, can override the information privacy rights of individuals. Victoria’s *Privacy and Data Protection Act 2014* (PDPA) contains new mechanisms that organisations can seek to use in cases where some flexibility around compliance with the Information Privacy Principles (IPPs) may be warranted. For more information on using these mechanisms please see the *Guidelines to public interest determinations, temporary public interest determinations, information usage arrangements and certification*. The guidelines can be accessed at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines.

Information sharing is not a stand alone concept. There are a number of other related concepts that influence – or are influenced by – information sharing, such as data matching activities and the new mechanisms referred to above. For the purposes of these guidelines, such related concepts will not be considered in detail. For advice on these and other topics of interest please refer to the material available on the CPDP website.

Improving information sharing practices first and foremost requires cultural change led by executives and public sector body heads. This necessitates an understanding of the key issues involved with information sharing, alongside an appreciation of the value that information sharing can derive for the public sector and for citizens.

---

\(^1\) ‘Personal information’ is defined in section 3 of the *Privacy and Data Protection Act 2014* 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* applies’.
Part 1: Introduction to information sharing

Information is the key to sound decision-making, to accountability and development; it underpins democracy and assists in combating poverty, oppression, corruption, prejudice and inefficiency. Administrators, judges, arbitrators, and persons conducting inquiries and investigations depend upon it; likewise the press, NGOs and individuals concerned to report on issues of public interest. Unwillingness to disclose information may arise through habits of secrecy or reasons of self-protection. But information can be genuinely private, confidential or sensitive, and these interests merit respect in their own right and, in the case of those who depend on information to fulfil their functions, because this may not otherwise be forthcoming.²

What is information sharing?

Although information sharing is a term that is not generally found in privacy legislation, the concepts that influence information sharing in practice form the foundation of privacy law. Information sharing in the public sector describes the collection, use and disclosure of personal information. Use and disclosure can take a variety of forms – it could be a single piece of personal information about an individual, or a data set that contains personal information about a group of individuals.³ A more comprehensive discussion of these concepts can be found in the Guidelines to the Information Privacy Principles, available at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines.

Information sharing can take place either between (disclosure) or within organisations (use). For example, government departments are often made up of multiple business units that are established under different pieces of legislation and have vastly different functions from each other – personal information collected by one unit for a particular purpose does not automatically entitle another unit to access that information. In such cases personal information can only be shared within the department if authorised by law.

The Department of Health and Human Services (DHHS) is one of Victoria’s largest government departments, made up of multiple portfolios including Housing, Families and Children, Mental Health, Disability, Ageing, and Sport and Recreation. Although each of these portfolios – and their contracted service providers – fall within the same department, the enabling legislation that governs each portfolio’s functions and activities may restrict the information that can be shared between business units. For example, personal information that is collected by the Office of Housing in connection with providing accommodation for a woman and her children cannot be disclosed to Child Protection simply by virtue of both offices being part of DHHS. Personal information can only be shared where there is a clear legal authority permitting, or requiring a disclosure for a particular purpose or function.

Information sharing can occur in a variety of formats, including by way of extending access to a repository of information to the receiving party; duplicating files for transfer, either electronically or in hard copy, or through data matching activities, among others.⁴ Information sharing may be reciprocal between participating parties, or could involve a one way exchange of personal information.

The collection principle – which states that personal information can only be collected if it is necessary for a specified function or activity – is the foundation of privacy law.⁵ The purpose for which information is collected is commonly referred to as the primary purpose. Information sharing will often involve the use or disclosure of personal information for a secondary purpose. There are important privacy considerations that arise when personal information is used or disclosed for a purpose other than for which it was originally collected. These will be discussed in more detail in a later section.

---

5 See Information Privacy Principle 1, Schedule 1, Privacy and Data Protection Act 2014.
Types of information sharing

Information sharing between parties can occur either systematically or on an ad hoc basis.

Systematic information sharing

Systematic, or ongoing information sharing activities, are usually the result of an arrangement between two or more organisations that agree to routine exchanges of information for an agreed purpose. Systematic sharing can involve parties pooling together their relevant information assets in a shared database, or simply transferring data via an agreed method and time on a routine basis. Ongoing information sharing activities should be governed by a written agreement between the parties – such as an information sharing agreement (ISA) – that sets out the relevant authorities and outlines the details of how the disclosures will take place. A detailed discussion of ISAs and the ongoing responsibilities associated with an agreement is provided in Part 4.

Ad hoc information sharing

In some instances, information sharing between parties may take place on a one-off basis. These requests for personal information might not be governed by a pre-existing agreement, arrangement or protocol, and require a considered decision to be made as to whether or not it is appropriate to share the information. It is also critical for the requesting organisation to ensure that they have the appropriate authority to collect the information they are asking for, including whether it is necessary for their functions. Ad hoc requests are commonly made in emergency situations, where urgent access to personal information is needed to facilitate a response.

In an emergency situation, a one-off request for residents’ information might be made to a Local Council by state emergency authorities, where that information is necessary to respond urgently to the situation. During a bushfire or flood for example, the personal information of residents in a particular vicinity could assist authorities to notify those who are in immediate danger. This type of ad hoc request may not require an ongoing information sharing arrangement, as the purposes for which the information is needed could be satisfied by a single exchange.

When an urgent request for access to information is received, the organisation may have to make a quick decision about whether or not to share the information. Nonetheless, there are important issues that they must still consider, including:

- whether they have the legal authority to share the information
- what the risks and benefits of sharing the information would be
- whether there are risks associated with not sharing the information, such as where an individual would be placed in danger were the information not shared
- whether appropriate privacy and data security measures are in place to protect the information, including during transfer.

A written record of all ad hoc requests for personal information should be made, regardless of whether the information was shared or not. In the case of systematic information sharing arrangements, the ISA serves as the record of each disclosure. For further information on what to include in a written record see the Checklist for sharing personal information contained in appendix D.

---

Importance of responsible information sharing

Responsible sharing of personal information is integral to upholding individuals’ rights to privacy. Privacy rights are not only preserved in the PDPA, but are also an important feature of the Victorian Charter of Human Rights and Responsibilities Act 2006 (the Charter), contained in section 13. All public sector organisations and their employees are required to act consistently with the Charter provisions in respect of making laws, developing policies and delivering services.

Responsible and appropriate information sharing is particularly important in the public sector. The relationship that individuals have with government is one that is defined by a power imbalance, where citizens are often compelled to engage with the public sector in order to receive services and benefits, such as obtaining a driver’s licence or receiving public health care. This is contrasted with the private sector – where, for example – customers can choose between alternative mobile phone providers if they are displeased with the service they are receiving.

Information sharing implies that personal information may be repurposed by the receiving party, potentially straying from the original purpose for which the information was collected. As such, it is important for organisations to be transparent about their information handling practices, and should provide the appropriate notice to individuals if their personal information is likely to be disclosed to third parties.

An unauthorised or unlawful disclosure of personal information in the public sector can result in a loss of privacy, and by extension, amount to a loss of trust in government. Additionally, a failure to communicate with other organisations and share information as appropriate when delivering services to individuals, can also affect the public’s confidence in government. Understanding the impacts of information sharing – both positive and negative – is vital to articulating public value.

Overview of the information sharing process

The information sharing process is made up of a number of steps that organisations should take before any sharing takes place, while the information exchange is occurring, and once an arrangement has concluded. Parts 3 and 4 of the guidelines outline this process in greater detail.

1. Know what personal information is to be shared and understand its value (overall importance).
2. Ensure you have the legal authority to collect/disclose the information, by first consulting your organisation’s enabling legislation, relevant confidentiality and secrecy provisions, and the PDPA.
3. Consider the relevant information privacy, protective data security and recordkeeping requirements, including those contained in internal policies and procedures.
4. Undertake a risk assessment, in consultation with the third party if necessary.
5. Seek legal advice or contact CPDP if in doubt about whether you can share the information.
6. Ensure that an ISA is in place for ongoing information sharing arrangements, and that all the relevant details are covered.
7. Ensure that mechanisms for monitoring and review of the agreement are in place, including incident management protocols.

---

Part 2: Information sharing benefits and barriers

This section outlines the benefits to the public sector and to the public at large that information sharing can bring about, as well as the barriers and challenges that can hinder the process.

Benefits of information sharing

The advantages of information sharing will in some situations be clearly evident, while in others there may be competing interests that need to be balanced, for instance where there is concern that a disclosure could negatively impact upon an individual’s safety. The benefit in disclosing personal information may not always be the dominant interest, and a balancing exercise will be necessary.

Benefits to the public sector

Decisions to share personal information between and within public sector organisations can result in benefits for the organisations themselves, and improve the way that government business is conducted.

Greater efficiency for organisations

There are a number of ways that information sharing can improve public sector efficiency. Disseminating information between government departments can allow information to be collected once and used multiple times (where lawful), negating the need for individual organisations to each collect the same information from individuals. This can save time, money and resources, while helping to break down ‘silos’ in terms of government departments operating independently of one another, and information assets being stored in isolation.

Confidence in data quality

Improved information sharing practices between organisations can help to verify the integrity of personal information, by enabling data custodians to confirm the accuracy of the information they already hold. Information received can also help to fill in any gaps in knowledge, building a more complete picture of an issue, ultimately leading to more sophisticated and authoritative decision-making and policy outcomes.

Greater trust and confidence in government

Information sharing can demonstrate a commitment to being transparent about what information organisations collect and use, and the practices they have in place for handling that information. Transparency and openness are highlighted as indicators of ‘good government’ (although the extent to which governments are open about their practices should be carefully weighed against any potential risks). This is reflected by one of the objects of the PDPA – “to promote the responsible and transparent handling of personal information in the public sector”. A commitment to openness and transparency can in turn secure greater trust and confidence in organisations from the perspective of:

- other organisations with whom information is shared, allowing them an insight into how the disclosing organisation carries out their information handling responsibilities
- the public, who hold an expectation that their information will be handled appropriately and that it will be shared with other organisations under the necessary circumstances.

---


10 Section 5(d), Privacy and Data Protection Act 2014.
Benefits to the public
Information sharing can also produce benefits to the individuals whose information is being disclosed, contributing to the creation of public value.

Convenience for citizens
The convenience of information being shared between agencies is something that many individuals can benefit from. Information sharing can negate the need for individuals to repeat the same information each time they access a service or change their personal details. This may prove time consuming and frustrating for individuals who often make use of a wide range of services, particularly where they expect government bodies to share this information about them.

The Australian Government’s myGov initiative allows users to access a range of services from Medicare, the Australian Tax Office and Centrelink via a single online account. For instance, users can change their contact details through the myGov portal, which means that they do not need to contact each body individually to do so; it is a routine, automated process that ensures information is accurate and up to date, while satisfying the public’s expectation that by giving up some of their information they will in turn benefit.

Better integrated services
Government departments typically operate in silos, divided by the specific policy and program areas for which they are responsible. Information sharing between organisations is one way in which silos can be broken down, referral processes simplified, and services better integrated to provide holistic, seamless solutions for individuals.

One of the benefits that better integrated services can achieve is the building of preventative models of service delivery – for instance, clients who are in danger of becoming homeless due to drug abuse can be identified as ‘at risk’ early on and benefit from preventative measures that service providers are able to implement based on the information received.

Enhanced protection for vulnerable people
A further benefit of public sector information sharing is that an increased flow of information can alleviate the demand upon individuals of having to provide the same information to multiple agencies. This is particularly beneficial for vulnerable people – such as victims of domestic violence – who may have suffered trauma or grief as a result of their experiences, where having to retell their story numerous times can make them feel revictimised.

Barriers to information sharing
There are a number of obstacles to public sector information sharing that are familiar all around the world. In some cases the barriers to information sharing are warranted, such as where there is no clear legal authority to disclose the information. In other situations obstacles exist as a result of a risk-averse culture within organisations that see requests for information automatically declined, even if there is a legal basis for the disclosure. It is important for organisations to understand which barriers within their organisations are real and which can be overcome, so that where there is a public value-creating purpose for information sharing, the appropriate disclosures are made. Some of the barriers are outlined below.

Constraints in enabling legislation
An organisation’s governing legislation may contain provisions that specify the circumstances under which particular types of information can be disclosed to other parties. As the starting point for organisations in determining what authority they have to share information, enabling legislation can also expressly prohibit information from being shared. Confidentiality and secrecy provisions contained therein override any permissions to disclose information under the PDPA or other legislation.
Constraints in privacy law

Privacy laws place important limitations around information sharing. The PDPA for example, specifies that personal information can only be used or disclosed for the primary purpose for which it was collected – unless one of eight exceptions apply – limiting the circumstances under which organisations can share information with other parties.\(^\text{11}\) This is commonly known as the *purpose limitation* principle. From the perspective of recipient organisations, the PDPA also places restrictions around the collection of information; unless the information is necessary for one of the organisation’s functions or activities, they may not have the authority to collect it.\(^\text{12}\)

In some cases however, privacy laws are *incorrectly* perceived as a barrier to information sharing, where data custodians wrongly assume that they are unable to disclose personal information, despite there being an explicit permission that allows information to be shared for that purpose. Experience suggests that it is easier for organisations to use privacy law as an excuse not to share, than it is to explore possible ways to enable the disclosure. The complexity of the relationship between privacy laws at different levels of government, and provisions within other pieces of legislation that deal with information sharing contribute to the perception that privacy law is a barrier.

Lack of leadership

The recognition that responsible information sharing is important to the public sector and to society must stem from a senior executive level within organisations.\(^\text{13}\) Often this awareness is lacking, resulting in frontline staff who are also unaware of how information sharing should occur, under what circumstances they are permitted to disclose personal information to third parties, and broader considerations of privacy and data security. This lack of leadership at senior levels can mean that in the absence of clear policies and procedures, information that should be shared may not be reaching the right people, and where it is not appropriate for personal information to be disclosed, unauthorised persons may be accessing it.

Cultural and institutional barriers

Cultural and institutional factors are often compelling influencers on an organisation’s information sharing practices.\(^\text{14}\) Some of the cultural and institutional barriers are set out below.

- **Risk aversion:** an overly cautious view of the risks associated with information sharing can prevent disclosures, even where there is a legal basis for the sharing to occur. There are rarely consequences for withholding personal information, but disclosing or collecting it inappropriately can have repercussions, deterring organisations from participating in information sharing at all.

- **Poor governance:** inadequate governance and accountability measures result in a lack of expertise and knowledge of how requests for personal information should be assessed, and what considerations need to be made when deciding whether or not to disclose. A lack of decision-making framework and poorly developed processes fail to guide staff in responding to requests for personal information.

- **Inadequate investment in resources:** outdated information technology systems and software that are not fit for purpose can make sharing information with other parties difficult.

Culture is often embedded into an organisation, which makes it difficult for change to occur and barriers to be overcome. To do so requires strong leadership that recognises the value in information sharing and acknowledges that potential risks must be balanced against the benefits that can be achieved; zero risk is never guaranteed.

---

11 See Information Privacy Principle 2, Schedule 1, Privacy and Data Protection Act 2014.
12 See Information Privacy Principle 1, Schedule 1, Privacy and Data Protection Act 2014.
Interoperability and compatibility issues
Organisations that wish to share personal information with each other often will not be operating on the same information management systems, and will format and store their information according to varying standards and prescribed methods. This can be challenging for the transmission and readability of data, and will often prevent legitimate disclosures from being made, simply because of such technical barriers.

Lack of trust
Engaging with another party to share personal information is necessitated by a trusting relationship. The disclosing organisation needs to be able to trust that the recipient will handle the information in accordance with privacy and security obligations, adhere to an ISA, and that they will only use the information obtained for the agreed-upon purpose. In some cases this level of trust may be lacking, particularly if the disclosing organisation has little evidence that the recipient will use the information appropriately and in the public interest.

Fear of financial or reputational damage
A further barrier to information sharing is the potential for the disclosing organisation to suffer financial or reputational damage if an inappropriate disclosure results in a privacy breach. When a request for personal information is received it can sometimes be difficult to ascertain the risks involved with making a disclosure, particularly where there are competing public interests at play. In order to ‘protect their turf’ and their information assets, some organisations may err on the side of caution and decide not to disclose, despite there being compelling benefits to allowing another party to access their information.
Part 3: Sharing personal information: A methodology

This part provides an overview of the factors to which organisations must give due consideration when it comes to information sharing. The first section looks at the steps that need to be taken to help organisations decide whether personal information can, and should be shared. The second section details the information privacy, data security and recordkeeping responsibilities that need to be considered if a decision to share personal information is reached.

Before you decide to share

When a request for personal information is received – whether for an ongoing or a one-off exchange – there are a number of initial steps that an organisation must take to assess whether there are grounds to collect the information or to make a disclosure. Each event must be considered contextually on a case-by-case basis by taking into account the unique circumstances of the request. Where there is a basis for information sharing to take place, the benefits of making a disclosure to the receiving party must be demonstrable, and should outweigh any potential adverse consequences.

There are four broad steps that organisations should take when making an assessment about whether or not to disclose information. Each of these is discussed in further detail below.

1. Know your information
2. Understand your authorising environment
3. Undertake a risk assessment
4. Seek advice if necessary

Step 1: Identify the type of personal information you are dealing with

The first step in assessing whether or not it is appropriate to share information is to know what type of information will be collected or disclosed. When making a request to an organisation for information, the requesting party should identify the data fields or categories of information they are seeking access to. If the disclosing organisation is unclear about what information is being sought from them they should seek to clarify this with the requesting party.

Categories of information could include personal information, sensitive personal information, health information, non-identifiable information, and de-identified information, among others. The type of information in question will determine the circumstances under which the information can be shared. For example, sensitive information will have a higher risk threshold – particularly around privacy and security – than non-identifiable data such as statistics. For a more detailed discussion around sensitive information see the Guidelines to the Information Privacy Principles available at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines.

Step 2: Understand your authorising environment

Whether or not an organisation has the ability to share or collect information is determined by their authorising environment. In the information sharing context, the authorising environment stems from legislative provisions that prescribe how information can and cannot be handled. These provisions are sometimes also detailed in policy and procedural documents that further describe an organisation’s authority, or limited ability to disclose information. It is important to note that express authorities within legislation to share information may only relate to particular types of information, and should not be relied upon as a broadly applicable permission to share. Both the disclosing organisation and the recipient of the information need to ensure that they can rely on an appropriate authority to participate in information sharing initiatives.

Legal authority to share

In assessing the authorising environment, organisations must first consult the legislation that is relevant to them – their enabling legislation. The PDPA is default legislation; the collection, use and disclosure provisions in the PDPA only apply to the extent that enabling legislation is silent on these matters. Enabling legislation will set out an organisation’s functions, as well as the powers the organisation may exercise to achieve the purposes of the legislation.

Authorities to share information can be represented by express obligations, express powers and implied powers.

**EXPRESS OBLIGATIONS**

Organisations may be legally required to share particular types of information with other named organisations.

**EXPRESS POWERS**

Enabling legislation may expressly permit the disclosure of information in certain circumstances for a particular purpose.

**IMPLIED POWERS**

Legislation may be silent on the issue of information sharing, but where sharing information would be reasonably necessary for the performance of an express provision, it may be implied that information can be shared.

Confidentiality and secrecy

Also contained within enabling legislation, organisations must consider any confidentiality or secrecy provisions by which they may be bound. Confidentiality provisions restrict the disclosure of information to authorised persons with a need to access that information. It is based on a trusting relationship between the disclosing and receiving parties, who share an understanding of the risk involved with the information being accessed by unauthorised persons. Secrecy provisions are provisions within an Act that prohibit the disclosure of certain types of information by individuals or entities, typically attracting penalties where the specified information is disclosed. Where a secrecy provision applies, information simply cannot be shared.

Confidentiality and secrecy provisions may not only apply to personal information but can extend to other types of information, such as sensitive business information.

19 UK Information Commissioner’s Office, Data Sharing Code of Practice, 2014, p. 11.
20 UK Information Commissioner’s Office, Data Sharing Code of Practice, 2014, pp. 11-12.
**Privacy law**

The authority to share personal information – or the prohibition on its disclosure – may be found in privacy law. The PDPA is default legislation, meaning that the IPPs apply only where other legislation is silent on privacy; enabling legislation always provides the overarching authority.

Under the PDPA, IPP 2 – Use and Disclosure – deals with information sharing in the public sector. IPP 2.1 states that “an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection”. There are eight exceptions to IPP 2.1 which permit the use and disclosure of personal information in limited circumstances. Some of these include:

- if the secondary purpose is related to the primary purpose of collection, and the individual would reasonably expect their information to be used or disclosed for the secondary purpose
- if the individual has consented to the use or disclosure
- for research purposes that are in the public interest, where it is impractical to seek the individual’s consent beforehand and the organisation reasonably believes that the recipient organisation will not disclose the information
- if the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual’s life, health, safety or welfare
- if the organisation has reason to suspect that unlawful activity has been engaged in, and uses or discloses the information to investigate the matter or to report the matter to relevant authorities
- if the use or disclosure is authorised by law.

**The Charter of Human Rights and Responsibilities**

Victorian public sector bodies have an obligation under the Charter when making decisions to consider the impact on the human rights of individuals. In addition to information sharing provisions contained within enabling legislation and privacy law, organisations must also ensure that a decision to share personal information (or not to share) is consistent with human rights under the Charter.\(^2\)

Giving due consideration to the Charter requires decision makers to:

- understand in general terms which of the rights of individuals may be relevant and whether those rights will be interfered with by the decision
- seriously turn their mind to the possible impact of the decision on individuals’ human rights and the implications of this for those affected
- identify the countervailing interests or obligations of the state
- balance competing private and public interests.\(^3\)

**Consent**

Obtaining an individual’s consent can be an attractive alternative for organisations wishing to share personal information. With an individual’s consent, personal information may be used and disclosed without the need to rely on another authority in the PDPA or another piece of legislation. However, relying on a consent-based model becomes problematic where organisations still intend to share personal information even where an individual has expressed a desire for their personal information not to be disclosed to third parties.

For example, where an information sharing provision in the PDPA or another piece of legislation expressly requires or permits personal information to be shared for a particular purpose, consent becomes meaningless if the individual does not in fact have a genuine choice. In these cases providing notice to individuals that their personal information will be disclosed to third parties may be appropriate, where relying on consent is not a viable option. Providing notice empowers and informs individuals, while promoting organisational transparency and accountability (although notice is not a solution where information sharing is not otherwise legally authorised).

---


\(^3\) Castles v Secretary of the Department of Justice & Ors (2010) VSC 181.
Other issues raised by a consent model include:

- the costs and resources associated with managing a consent model
- whether consent is relevant for a one-off disclosure only or can be relied upon for future disclosures
- whether consent can be withdrawn at a later time once information has already been shared
- the extent to which individuals are able to give informed consent, given that consent can easily be collected through a ‘check box’ exercise
- the appropriateness of relying on consent in situations where it is lawful to disclose personal information for a greater public interest such as public safety or law enforcement.  

**Step 3: Undertake a risk assessment**

Once the authority to collect or disclose personal information has been established, a risk assessment should be undertaken before a decision is made about whether or not to engage in information sharing. Part of a risk assessment process should be a consideration of ‘risk appetite’. Organisations should determine, based on the potential risks they identify, how much risk they are willing to accept and be held accountable for. For example, where there are threats to a disclosing organisation that outweigh the likely benefits of sharing personal information, they may decide to deny the disclosure request.

The relevant risks will be different for each organisation. Some of the common risk factors are outlined below.

**Necessary, proportionate, timely and secure**

Before deciding whether or not to collect personal information or make a disclosure, organisations need to assess whether the information sharing is:

- **Necessary** to achieve the defined purpose for which the information will be used – could the same purpose be achieved without the personal information? Could personal information be de-identified before being disclosed whilst still achieving the same desired outcome?
- **Proportionate** to the purpose and the desired outcome of using the personal information – does the public interest in sharing the information outweigh any other public interests such as privacy or safety? Is the amount of personal information to be shared proportional to its intended use?
- Conducted in a **timely** manner – is the timing of the disclosure appropriate to when the information is needed?
- Undertaken in a **secure** manner – are the security measures in place proportionate to the value of the information being disclosed?  

**Interoperability and compatibility**

Often framed as a physical barrier to information sharing, poor interoperability between parties’ systems and processes can pose a risk to timely, secure information sharing, and result in financial loss to organisations that spend time attempting to merge different systems. Prior to entering into an information sharing arrangement, the extent of any interoperability or compatibility issues needs to be evaluated.

Some of the factors that may need to be overcome in order to ensure interoperability include:

- different information technology systems
- different data formats
- inconsistent standards for recording and maintaining the accuracy of information
- inconsistent data retention periods and deletion protocols
- different privacy and data security obligations, particularly where personal information is shared between jurisdictions.

---

**Privacy impact assessment**

Before a decision is made to participate in information sharing initiatives, organisations should undertake a privacy impact assessment (PIA). A PIA is a tool used to assess an organisation’s compliance with their information privacy obligations and requirements, and to identify any potential privacy risks that may arise if an initiative was to be implemented in its current form. Undertaking a PIA is essential for proposed information sharing arrangements involving personal information, given that they are often complex and affect many of the IPPs. Once complete, a PIA can help organisations to identify risk mitigation strategies. In some cases however, a PIA may reveal that an initiative should not go ahead because the information sharing is not authorised or the privacy risk involved is too great.

A PIA should be undertaken by each party involved in an information sharing arrangement, as the legal authorities, potential risks and mitigation strategies will differ for the disclosing and receiving organisation. Organisations may wish to undertake separate PIAs, or may decide there is value in undertaking a joint PIA. A joint PIA should be sure to distinctly set out each party’s obligations and compliance with the IPPs.


**Risk in not sharing**

In addition to assessing the risks of disclosing personal information, it is critical that consideration is also given to the potential risks of not sharing the information that is requested. The risks associated with information sharing are symmetrical – in some cases it may cause harm to share, but in others a greater harm may result if the information cannot be accessed by the party requesting it. This requires that the disclosing organisation make a judgement based on the purpose for which the information will be used and its intended outcome, balanced against the risk that may result from a failure to achieve that outcome.

**Step 4: Seek advice where necessary**

The final step in assessing whether or not to engage in information sharing is to seek advice on the matter where necessary.

**Legal advice**

When a request for personal information is received and it is not clear as to whether a disclosure is permitted under law, an organisation’s legal team should be consulted. For example, where there is ambiguity in relation to whether or not any of the exceptions to IPP 2.1 apply in a particular matter, the legal department can offer advice on whether an information sharing practice would be consistent with legal obligations. Organisations should also seek legal advice if it is unclear whether or not they have the authority to collect information for a particular purpose.

**Advice from the Commissioner for Privacy and Data Protection**

Organisations can also seek privacy and security advice from CPDP in relation to an information sharing initiative. In some cases two or more organisations who are party to a forthcoming information sharing arrangement may receive conflicting legal advice with regards to whether a proposed information sharing practice is privacy-compliant. Under the PDPA an organisation can seek certification from the Commissioner that their intended act or practice is consistent with the IPPs. If certified, the organisation can be assured that they are upholding their privacy obligations under the PDPA. For more information on the certification mechanism see the Guidelines to public interest determinations, temporary public interest determinations, information usage arrangements and certification.

---


If you decide to share

This section looks at the information privacy, protective data security and recordkeeping obligations that need to be met if a decision is made to share information.

Information privacy

The IPPs set out the minimum privacy protections that Victorian public sector organisations must adhere to. In addition to IPP 2 – the requirements of which have already been discussed – there are a number of other IPPs that are important to information sharing:

• **IPP 1 – Collection:** IPP 1 deals with the collection of personal information. Both disclosing organisations and recipients of information have obligations under this IPP:
  - IPP 1.1 states that an organisation must not collect personal information unless it is necessary for its functions or activities. This means that when seeking access to personal information an organisation must have a clear purpose for which they will use the information, which relates to the performance of one of their functions. Further, when disclosing personal information to a third party, an organisation must only share the minimum amount of information necessary for the identified purpose.
  - When collecting personal information organisations are required to notify an individual of the matters set out in IPP 1.3, which include the identity of the organisation and how it can be contacted, the purposes for which the information will be collected, any law that requires that collection, and to whom the individual’s information may be routinely disclosed. Where an ISA is in effect and an individual’s information forms part of the routine disclosure, the individual must be notified of this by the original collecting organisation.

• **IPP 3 – Data Quality:** IPP 3.1 requires organisations to take reasonable steps to ensure that the personal information they collect, use and disclose is complete, accurate and up to date. Organisations should regularly review the personal information they hold and ensure that it is accurate before disclosing it to a third party. This may form part of a data custodian’s role.

• **IPP 4 – Data Security:** Privacy and data security are intrinsically linked concepts – without security privacy cannot be assured. IPP 4.1 requires organisations to take reasonable steps to ensure the personal information they hold is protected from misuse and loss, and unauthorised access, modification or disclosure. In practice, IPP 4.1 requires that sufficient security measures are implemented to prevent personal information from being disclosed where it is not authorised, and to ensure the security of information during transfer.

• **IPP 9 – Transborder Data Flows:** In some cases parties to an ISA may be located in different jurisdictions. IPP 9.1 is intended to ensure that personal information is only transferred across borders where the receiving organisation is bound by privacy principles that are substantially similar to the IPPs (or where some other permission applies). This assures individuals that where their information is sent interstate or overseas, privacy protections follow their information. IPP 9 has become increasingly important with the use of cloud computing and offshore data storage. Authoritative guidance relating to cloud computing is available at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-background-papers.
Protective data security

There are three overarching principles that guide how organisations should implement data security measures to protect the information they hold. These principles, which should be applied step-by-step, are relevant not only to information sharing initiatives involving personal information, but should be applied to all information assets. The three principles are outlined below.

Understand your information

The first step in applying appropriate data security measures is for organisations to understand what type of information they are dealing with, as this will determine the value of the information and subsequently, the controls that need to be put in place to protect the information.

Understand the value of the information

Understanding the value of information is underpinned by the ‘CIA triad’ – confidentiality, integrity and availability. This is a commonly used framework for assessing the threat level to an organisation were the confidentiality, integrity or availability of the information to be compromised. Understanding the likely consequences of a security incident will determine the value of that information to the organisation. Once value has been established, the appropriate data security controls can be applied to the information to protect it throughout the information sharing process and minimise the potential for a security breach.

Apply the appropriate security controls

Putting in place controls to minimise unauthorised access or disclosure is not predicated on designing a foolproof system that will never result in an incident. Rather, robust controls should be implemented to address any known risks that have been identified.

The Victorian Protective Data Security Standards (VPDSS) underpin this thinking. The VPDSS – currently in draft form – are made up of standards that set out the mandatory security requirements for the protection of all public sector data, which includes but is not limited to, personal information. The VPDSS cover five core security domains: governance, information security, ICT security, personnel security and physical security.

Within the information security domain is a standard relating to information sharing. This standard states that ‘agencies or bodies must ensure that security measures are applied prior to the sharing of public sector data… to enable secure information sharing practices between parties and to prevent the unauthorised sharing of public sector data’. This standard articulates a Security by Design (SbD) approach to information sharing, a concept discussed further in Part 5.

When entering into an information sharing arrangement Victorian public sector organisations must ensure that the receiving organisation can uphold comparable standards to the VPDSS. For a more detailed discussion of the VPDSS and the information sharing standard, please visit the CPDP website.

---

Recordkeeping

Public sector employees have an express obligation to create full and accurate records of all of their work-related activities and decisions, which includes any decisions relating to information sharing. The responsibilities that organisations have towards managing records are contained within the PDPA and the Public Records Act 1973 (PRA), which is administered by the Public Record Office of Victoria (PROV).

By its very nature recordkeeping involves elements of both privacy and security, many of which have already been discussed. For example, ensuring data quality is important for upholding good privacy, as well as for keeping accurate records; secure storage is also critical from both data security and recordkeeping perspectives. Recordkeeping obligations should be considered throughout the entire information lifecycle.

Documenting decisions

For ongoing or systematic information sharing initiatives, the ISA will serve as the record for the disclosures that follow. For ad hoc information sharing, documentation must be created for each request, even in cases where a decision is made not to share. This should be accompanied by the reasoning for the decision. It is important that a standardised, systematic approach is taken to creating records to ensure consistency; internal policies and procedures should outline a coherent methodology for documenting decisions.

Documenting decisions and authorities to share information is also crucial from an accountability perspective. In the event of a privacy complaint or breach, a complete record of a decision made to disclose information can serve to justify an organisation’s actions.

For suggestions on what information should be recorded for one-off requests see the Checklist for sharing personal information contained in appendix D.

Disposal of records

In Victoria records must be kept and disposed of in accordance with the retention and disposal authorities set by PROV, which specify for how long particular types of records must be retained, and how they are to be disposed of. IPP 4.2 also speaks to this requirement, stating that organisations must destroy or permanently de-identify personal information if it is no longer required for a particular purpose.

When entering into an information sharing arrangement receiving parties should identify for how long they may be required to retain information, and ensure that the disclosing organisation is aware of this time period. This upfront identification of how long information will be kept can help to improve transparency and trust between organisations.

---

31 Public Record Office Victoria, Recordkeeping Responsibilities for Public Sector Employees, 2015.
33 See http://prov.vic.gov.au for a list of all current Records Authorities.
Part 4: Information sharing agreement and ongoing responsibilities

Information sharing agreements

In cases where a decision has been made to engage in an ongoing information sharing initiative, organisations should formalise their arrangement. An ISA is a formal, written agreement or protocol that sets out the circumstances under which an exchange of information will routinely take place. An ISA must be approved and signed off by all parties involved.

Organisations must ensure that they have the capacity to fully operationalise an ISA. This means that the appropriate resources need to be allocated to implement each component of the agreement, employees must be aware of their obligations, and need to be equipped with the necessary skills to execute their responsibilities.

An ISA should contain:

- the details of the participating organisations
- the purpose for which the information will be shared
- what information is to be shared, and the value of that information
- the legal basis for sharing the information
- how the information will be shared and the security measures that organisations will put in place to ensure secure transfer
- how the information will be stored, including security measures to protect the information from unauthorised access, amendment, use or disclosure
- which organisation(s) maintain ownership of the information
- the position of the staff member within organisations who will act as data custodian
- how long the information will be retained and how it will be destroyed
- the dates and times that the information sharing will take place
- notification of when the agreement will be reviewed, or terminated if known.

An ISA differs from an information usage arrangement (IUA) in a number of ways. IUAs were introduced into the PDPA along with other new mechanisms, allowing organisations to depart from one or more of the IPPs where the Commissioner agrees that there is a substantial public interest in them doing so. An IUA can be made in respect of any act or practice involving the handling of personal information – it is not specifically an information sharing instrument.

An ISA outlines the nature of an agreement between two or more parties in relation to how they intend to share information; it will specify each party’s legal requirements, but does not allow flexibility in terms of complying with privacy obligations. ISAs should be in place for all information sharing initiatives, whereas IUAs will only be approved in circumstances where non-compliance with privacy principles is warranted for a specified information sharing activity.

Ongoing requirements and responsibilities

Once an ISA is signed, participating organisations have ongoing responsibilities to ensure that the terms of the ISA are upheld, and that in practice, the ISA facilitates effective and responsible information sharing.

34 UK Centre of Excellence for Information Sharing, Information Sharing Agreement.

35 An IUA cannot be made in respect of IPP 4 – Data Security or IPP 6 – Access and Correction. See the Guidelines to public interest determinations, temporary public interest determinations, information usage arrangements and certification for more information.
Oversight and monitoring
It is important that monitoring and oversight of the way in which the disclosed information is handled by the receiving party occurs regularly. This can assure the disclosing organisation that the personal information they provided is being used only for the intended purpose, and that it is subject to appropriate security and access controls. Mechanisms for monitoring may be built into an ISA so that all parties involved are clear as to how oversight will occur. For example, the receiving party may be required to provide a report to the disclosing organisation annually, outlining how the personal information has been used.

Periodic review
The ISA should contain measures for the periodic review of the terms of the agreement. As legislative, policy and program circumstances change, the ISA will need to be updated to reflect the new authorising environment.

Secure destruction
Public sector organisations have an obligation under IPP 4.2 of the PDPA to ensure that information is securely destroyed or de-identified once it is no longer required for any purpose. This requirement needs to be balanced against the retention and disposal authorities set by PROV, which specify for how long information must be retained by public sector organisations. The method of destruction should be commensurate to the value of the information, ensuring that the confidentiality of information is not undermined.

Incident management protocols
Organisations should have in place protocols for receiving and responding to incidents that result from a privacy or security breach. It is good practice to establish pathways for managing incidents or complaints that stem from other organisations as well as from the public, who may suffer adverse effects if their information is handled inappropriately.
Part 5: Establishing an information sharing culture

An information sharing culture is an important underpinning feature of effective information sharing. In the absence of an inherent culture that values and promotes the sharing of information between public sector organisations, efforts to share information can be stifled by a lack of understanding of the key considerations.

This part considers the underlying principles that need to be established and embedded into organisations to enable effective, responsible and privacy-protective information sharing. Outlined below are the fundamental principles that need to be established to foster an information sharing culture.

Understanding competing interests

In every information sharing transaction there will be competing interests between the participating parties that need to be considered and balanced. For example, the organisations that are disclosing and receiving the information each may have different authorities to collect and share the information in question – one might be bound by enabling legislation that contains a confidentiality provision, while another could have powers as a law enforcement agency to obtain the information regardless of any other information handling provision.

Public interests can also be in direct competition with each other. Citizens’ expectations of collaborative, integrated public services need to be balanced against information privacy requirements. In some cases the interest in sharing personal information to deliver better services may outweigh the interest in withholding access to the information, while in other cases it might not. A general understanding of the range of positions of key stakeholders can serve organisations well in making decisions about whether or not to share information.

Governance and accountability

Each party to an information sharing arrangement should have a designated role within the organisation that is responsible for the overall governance of information sharing, and who remains accountable for the disclosures that take place. By demonstrating a commitment to responsible information sharing, strong leadership can facilitate cooperation between parties and help to establish trusting relationships. Good intentions to share personal information appropriately can easily be undermined by a lack of leadership and expertise.

Establishing a governance framework that sets out the authorities, processes and responsibilities for information sharing can serve as a useful tool for staff at all levels within an organisation when issues around information sharing arise. A governance framework can strengthen staff understanding of information sharing, build confidence that personal information will be shared appropriately by authorised staff, and embed information sharing practices into organisational culture.

The mechanisms and tools that form part of an information sharing governance framework should include:

- an overview of the overarching authorising environment, including legal authorities, obligations and prohibitions on disclosing information
- standards around how information is formatted and stored
- data custodianship guidelines that set out the rules and responsibilities of data custodians when maintaining data sets
- processes for assessing disclosure requests
- procedures for documenting requests and disclosures
- identification of potential or actual risks along with mitigation strategies
- dispute resolution processes
- monitoring of access logs and performance criteria.

Openness and transparency

Improved openness and transparency is a benefit of public sector information sharing, yet these concepts are also important underlying factors that need to be embedded into organisations in order for effective information sharing to take place. An organisation that is open about their information handling practices – including what type of personal information they collect from individuals, how they manage privacy and security obligations, and how they use individuals’ information on a day-to-day basis – as is required of organisations under IPP 5 – will be more likely to earn the trust of stakeholders with whom they wish to share information, when the time comes for this to occur. Transparency can also assure the public that their personal information will be handled appropriately.

Staff training and awareness

Establishing an information sharing culture is predicated on informed, knowledgeable staff who have the capacity and understanding to make the right decisions. Providing training and ongoing awareness activities is critical for ensuring that staff:

- understand what information sharing entails, and when personal information can and should be shared
- know who within the organisation has the ability to authorise a disclosure
- understand how information privacy, data security and recordkeeping obligations inform information sharing practices, and the responsibilities for meeting these at an individual level (such as knowing when to undertake a PIA)
- are able to meet reasonable expectations of individuals and oversight bodies regarding how personal information is handled.

Adopting Privacy by Design and Security by Design

Privacy by Design (PbD) is a methodology that enables privacy to be ‘built in’ to the design of information systems and business processes. It aims to ensure that privacy is considered before, and throughout, the development and implementation of all initiatives that involve personal information. By doing so, potential privacy risks that may arise can be identified and mitigated upfront, promoting a proactive approach to protecting privacy, rather than a remedial one. PbD is based on seven foundational principles, outlined in the table below.

SbD emerged out of the PbD methodology. A similar theory underpins SbD, which promotes a holistic approach to designing systems and processes with security in mind from the outset, minimising the potential for a security breach to occur. SbD substitutes the seven foundational principles of PbD for security-based principles. The table below sets out the foundational principles from both a privacy and security perspective.

---

40 Privacy by Design in a concept that was first developed in the 1990s by the former Privacy and Information Commissioner of Ontario, Canada, Dr Ann Cavoukian. Since then it has been adopted by both private and public sector bodies all over the world. The http://privacybydesign.ca website contains a wealth of information on Privacy by Design. CPDP has also released guidance material on operationalising Privacy by Design for the Victorian public sector, available at http://cpdp.vic.gov.au.
Adopting PbD and SbD can foster an organisational culture that values information privacy and security, and the benefits of upholding core privacy and security principles. This in turn can influence how privacy and security are managed throughout information sharing initiatives. With PbD and SbD approaches assurance can be given that when personal information is disclosed to another party, the relevant considerations have already been taken into account and embedded into the information sharing process.
Conclusion

Information sharing is driven by a complex web of legislative requirements and restrictions, competing interests, interdependencies and ethical considerations. The complexities that governments are faced with when trying to navigate the information sharing environment have contributed to an apprehensive culture that has left the Victorian public sector lacking confidence to pursue joined-up government through information sharing.

These guidelines are intended to provide public sector organisations with a fundamental understanding of the steps that need to be taken to share personal information effectively and lawfully, beginning with building an information sharing culture. This guide has specifically focused on the implications of information sharing on three key information management domains – information privacy, protective data security and recordkeeping.

Information sharing in the public sector can produce significant benefits to both governments and to the public. It is vital that the key issues around information sharing are understood by those responsible for making decisions about collecting or disclosing information. Common misconceptions that privacy law is a barrier to information sharing need to be overcome, along with insufficient governance and leadership within organisations that stifle sharing in circumstances where it would be legitimate and appropriate.
Appendix A – Glossary of key terms

**Availability**: assurance that authorised persons are able to access defined information for approved purposes at the time they need to do so.

**Charter of Human Rights and Responsibilities (the Charter)**: sets out the basic rights, freedoms and responsibilities of all people in Victoria. The Charter requires public authorities and people delivering services on behalf of government to act consistently with the human rights in the Charter.

**Confidentiality**: limiting access to information to authorised persons for a specified purpose. The confidentiality requirement is determined by considering the likely consequences if the information were to be accessed by an unauthorised person.

**Confidentiality provision**: a provision within an Act that restricts the disclosure of information to those with a need to know.

**Contracted service provider (CSP)**: a person or body who provides services under state contract.

**De-identified information**: information from which individual identifiers have been removed so that an individual cannot be directly identified from that information.

**Health information**: defined in the Health Records Act 2001 as information or an opinion about the physical, mental or psychological health (at any time) of an individual that is also personal information (see Health Records Act 2001 for full definition).

**Health Records Act 2001**: Victorian legislation that regulates the collection and handling of individuals’ health information.

**Information privacy**: refers to an individual’s right to determine for themselves who has access to their personal information and how it is used.

**Information Privacy Principles (IPPs)**: refers to the 10 principles contained in Schedule 1 of the Privacy and Data Protection Act 2014 that set out the minimum requirements for the collection and handling of personal information in the Victorian public sector.

**Information sharing**: describes the process of disclosing information from one party to another, who subsequently collects that information.

**Information sharing agreement (ISA)**: a written agreement between two or more parties that governs information sharing activities. An ISA should include the purpose for which information sharing will take place, the legal authority for information sharing, how the sharing will take place, and the roles and responsibilities of each party.

**Information usage arrangement (IUA)**: an arrangement that sets out acts or practices for handling personal information, which either modifies the application of one or more of the IPPs or a code of practice, provides that the practice does not need to comply with one or more of the IPPs, or permits handling personal information for the purpose of an information handling provision.

**Integrity**: assurance that information can only be created, amended or deleted by authorised means, and that it is valid and correct.

**Non-identifiable information**: information that have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified.

**Personal information**: defined in the Privacy and Data Protection Act 2014 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 applies.

**Privacy and Data Protection Act 2014 (PDPA)**: Victorian legislation that is designed to protect all public sector data, including personal information and law enforcement data. The PDPA replaced the Information Privacy Act 2000.
**Privacy by Design (PbD):** a methodology that enables privacy to be ‘built in’ to the design of information systems and business processes, ensuring that privacy is considered before, and throughout, the development and implementation of all initiatives that involve personal information.

**Protective data security:** a risk management process designed to safeguard information assets by putting in place appropriate security measures that are proportionate to likely threats. Protective data security is also commonly referred to as ‘data protection’ or ‘information security’.

**Public Records Act 1973:** Victorian legislation that established the Public Record Office of Victoria (PROV) for the sound management of public records.

**Public sector data:** defined in the *Privacy and Data Protection Act 2014* as any information (including personal information) obtained, received or held by an agency or body to which Part 4 of the Act applies.

**Public value:** describes the value that organisations contribute to advancing the interests of the public.

**Secrecy provision:** a provision within an Act that prohibits the disclosure of information, and which may attract penalties if breached.

**Security by Design (SbD):** a methodology that enables security to be ‘built in’ to the design of information systems and business processes, ensuring that security is considered before, and throughout, the development and implementation of all initiatives that involve personal information.

**Sensitive information:** defined in the *Privacy and Data Protection Act 2014* as information or an opinion about an individual’s racial or ethnic origin; or political opinions; or membership of a political association; or religious beliefs or affiliations; or philosophical beliefs; or membership of a professional or trade association; or membership of a trade union; or sexual preferences or practices; or criminal record – that is also personal information.

**Victorian protective data security standards (VPDSS):** the standards issued by the Commissioner for Privacy and Data Protection under section 92 of the *Privacy and Data Protection Act 2014* for the protection of public sector data.
Appendix B – References

Victoria
Privacy and Data Protection Act 2014 (Vic).
Public Record Office Victoria, Recordkeeping Responsibilities for Public Sector Employees, 2015.

Australia

Canada

UK
UK Centre of Excellence for Information Sharing, Information Sharing Agreement.
UK Information Commissioner’s Office, Data Sharing Code of Practice, 2014.
Appendix C – Information sharing flowchart

Before you decide to share:

Identify the type of information:
- Is it personal information?
  - Yes
  - No
- Is it health information?
  - Yes, consult the Office of the Health Services Commissioner.
  - No
- You have no obligations under Part 3 of the Privacy and Data Protection Act. Share the information appropriately.

Ensure you have the legal authority to share:
- Is the sharing authorised in your program’s enabling legislation?
  - Yes
  - No
- Is the sharing authorised under IPP 2 of the Privacy and Data Protection Act?
  - Yes, reconsider the need to share and seek legal advice if required.
  - No
- Do you have the individual’s consent to share?
  - Yes
  - No

Undertake a risk assessment:
- Is the sharing necessary, proportionate and timely to achieve the defined purpose?
  - Yes
  - No
- Can the information be de-identified?
  - Yes
  - No
- Would a public interest determination or information usage arrangement be appropriate?
  - Yes
  - No
- Reconsider the need to share.

Consult the Office of the Commissioner for Privacy and Data Protection:
- Does the receiving party have comparable privacy and data security obligations in place?
  - Yes
  - No
- Reconsider the need to share.

Consult the Office of the Commissioner for Privacy and Data Protection:
- Does the receiving party have comparable privacy and data security obligations in place?
  - Yes
  - No
- Reconsider the need to share.

You have no obligations under Part 3 of the Privacy and Data Protection Act. Share the information appropriately.

Completing a Privacy Impact Assessment (PIA) will assist you to answer the questions below. Please consider undertaking a PIA if you have not done so already.
Appendix D – Information sharing checklist

Ask the right questions first

Do you have the legal authority to share?
Organisations need to consider their own enabling legislation, as well as any other legislation they are required to comply with, including the Privacy and Data Protection Act 2014.
Key points to consider:
• The types of organisations involved
• Any relevant functions or powers of your organisation
• The nature of the information you have been asked to share (for example was it given in confidence or protected by confidentiality provisions in legislation, is it sensitive information?)
• Any legal obligation to share the information (for example a statutory requirement or a court order)
• Is the purpose of sharing the information in accordance with Information Privacy Principle (IPP) 2?

Is the sharing justified?
Key points to consider:
• What is the purpose of the sharing?
• Could the objective be achieved without sharing personal information?
• Does the program share the least amount of personal information necessary to achieve the purpose?
• Is it feasible for the data to be de-identified prior to being shared?
• Is the sharing proportionate to the issue you are addressing?
• Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

If you decide to share
Key points to consider:
• Only share the necessary information that you have legal authority to share
• Ensure information is shared securely
• Ensure appropriate documentation of your sharing
• If you decide to share personal information and the proposed sharing will modify one or more of the IPPs (except IPP 4 and 6) it may be appropriate to consider an information usage arrangement, public interest determination, or temporary public interest determination.
Record your decision

For ongoing systematic sharing of personal information

It is good practice to have an information sharing agreement (ISA) in place for routine information sharing arrangements. As well as considering the key points above, your ISA should cover the following issues:

- The parties that will be involved
- The specific purpose of the information sharing arrangement
- The relevant legal authorities to share and collect information
- A specific description of the personal information covered by the agreement
- A description of how the personal information will be collected, used and disclosed
- Measures to ensure adequate security is in place to protect the data
- The arrangements that are in place to provide individuals access to their personal information upon request
- Agreed common retention periods for the information
- Processes to ensure secure deletion of information takes place
- Any restrictions on the receiving party sharing the information further, or using it for additional purposes
- Mechanism for reviewing the agreement periodically.

For one off requests for personal information

Record your information sharing decision and your reasoning, whether or not you shared the information.

If you share the information you should record:

- What information was shared and for what purpose
- Who it was shared with
- When it was shared
- Your justification for sharing
- Whether the information was shared with or without the consent of individuals.