How to use this document

This case study considers a common type of outsourcing arrangement: where a Victorian public sector (**VPS**) body shares its client and case management database with its funded contracted service providers. This case study assumes that the VPS body is subject to both Parts 3 (Information Privacy) and 4 (Protective Data Security) of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

This case study is intended to be read in conjunction with the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*, which provide more detailed implementation guidance. You may also wish to refer to the *Short form Model Terms for Contracted Service Provider agreements.*

Scenario

You are part of the operations team for a client-facing division (your **Division**) in a Victorian government department (your **Organisation**).

Your team delivers services to the public, working with a range of non-government contracted service providers (**CSPs**). While your team retains overall responsibility for each client, the CSPs deliver parts of the overall service to the client. Your Division also co-ordinates with other service divisions within your Organisation, in cases where the individual is a client of both services divisions.

Your Organisation’s technology services team will establish a client and case management system (the **Case Management** **System**) that will be shared with the CSPs. The Case Management System will have client files that can be accessed and updated by both your team and CSP staff. CSPs access the Case Management System by a web portal.

The Case Management System will also integrate information from databases of other divisions in your Organisation. It can be searched by other service divisions through a basic profile to allow them to identify common clients so that your Organisation can co-ordinate service delivery across divisions.

You are invited to comment on functional requirements needed for the Case Management System portal.

What are your Organisation's responsibilities in this scenario?

The client files in the Case Management System will contain "personal information" under the PDP Act. Consequently, the Information Privacy Principles (**IPPs**) apply:

*The IPPs require your Organisation to clearly inform clients about how their client files will be used, and who will have access to their client files. The IPPs also require your Organisation to take reasonable steps to ensure that the client files remain accurate and up-to-date, and that there are appropriate arrangements in place to allow clients to exercise their rights to request access to (or correction of) the information in their client files.*

The Case Management System is a "public sector data system" under the PDP Act, and the client files in the Case Management System are "public sector data". Consequently, the Victorian Protective Data Security Standards (**VPDSS**) also apply:

*The VPDSS requires your Organisation to keep track of the types of information and records that are held or managed by the Organisation, and the location of these records. The VPDSS also requires your Organisation to implement standardised governance procedures to ensure that new databases and file repositories can be assessed for risk and protected in a manner that is consistent with other similar databases and repositories. When setting up a new database or file repository, you should ensure that the relevant business functions in your Organisation are notified.*

In this scenario, your Organisation manages the overall client relationship and is primarily accountable for the client files in the Case Management System. While your Organisation may delegate specific roles and responsibilities to the CSPs, your Organisation remains accountable for ensuring that the client files are accurate and are only accessed by authorised personnel for authorised purposes on a "need to know" basis. The Organisation is also responsible for managing "lifecycle" issues, such as determining how long client files should be retained in the Case Management System before they are archived.

Complying with the IPPs and VPDSS requires a co-ordinated effort from many different stakeholders in your Organisation including the operational service delivery teams, records management, IT operations and support, IT security, legal, and compliance / audit teams.

Breaching privacy and data security controls can have serious consequences. For example, insufficiently managing shared databases can lead to inaccurate, incomplete, or out of date client information which adversely impacts the quality of service delivery and decision making.

Key privacy and data security risks in this scenario

**Overview**

Discussed below are eight common privacy and data security risks that should be considered when your Organisation shares the management of an electronic client file with a funded CSP. The case study suggests risk mitigation strategies during the (i) pre-contract (due diligence / requirements gathering); (ii) contracting; and (iii) operational phases.

**Risk 1: Clients may not understand the relationship between the CSP and the Organisation**

***Description of risk***

The information that clients give the CSP is added to the Case Management System, which is shared by your Organisation and the CSPs. This effectively results in frequent and detailed information sharing between the CSP and your operations team.

There is a risk that the client may not understand the relationship between the CSP, your Organisation and other divisions in your Organisation that may operate with different branding. The client may be surprised when staff from your Organisation raise issues that the client has only discussed with CSP, or that your operations team shares profile information about them with other divisions within your Organisation.

This risk is primarily managed by preparing a written "privacy collection notice" that explains to clients how their client file will be managed, and who it will be shared with. Your Organisation's privacy officer can help you to prepare the privacy collection notice.

(*Key PDP Act references: IPP 1.3, 1.5 and 10*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Prepare an information flow diagram that sets out how information in client files will be used and shared through the Case Management System (including identifying common client relationships with other service divisions);
* After mapping information flows, consider if your Organisation’s Information Asset Register should be updated;
* Consult with your Organisation's privacy officer to develop a privacy collection notice based on the information flow diagram. The privacy collection notice should address the requirements set out in IPP 1.3 in the PDP Act; and
* Work with your Organisation's technology services team to build privacy cues / prompts into the Case Management System workflows (e.g. a pop-up that reminds the user to provide the client with a privacy collection notice when the user tries to create a new client file on the system).
 |
| Contract terms | * The CSP should be required to provide the privacy collection notice to clients; and
* Your Organisation should have contractual rights to monitor and audit the CSP's compliance with this requirement and may require the CSP to notify your Organisation where there is a breach of this requirement.
 |
| Operational phase | * Ensure that the privacy collection notice is provided to the CSP, and that your operations team also adopts the new privacy collection notice; and
* Monitor the CSP's compliance through periodic performance reviews.
 |

**Risk 2: CSP staff may not understand their roles and responsibilities in managing client files**

***Description of risk***

To ensure the integrity of the Database, your operations team will need to work with the CSP to ensure that both parties consistently record and manage information in the Database. For example:

* the types of information and documents that are appropriate to store in the client file;
* security controls applied to client files (e.g. confidentiality settings and protective markings);
* how case management roles are allocated within the Case Management System; and
* that the terminology and file noting practices used by your team are compatible with those used by the CSP's staff.

Your operations team should also ensure that the CSP and its staff have a clear understanding of what constitutes "Acceptable Use" of the Case Management System, to reduce the risk of CSP staff using the Case Management System for unauthorised purposes (whether intentionally, or inadvertently).

(*Key PDP Act references: IPP 1, 2.1, 3, 4 and 6; VPDSS 4, 5, 8 and 10*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Develop a shared responsibility model that sets out the respective roles and responsibilities of your Organisation and the CSP in managing the shared client file;
* Consider developing a policy and procedures document for the Case Management System that can be used by your operations team and shared with CSP staff; and
* Develop an appropriate on-boarding training program for CSP staff and decide who is responsible for conducting this training.
 |
| Contract terms | * Allocate relevant roles and responsibilities to the CSP, in accordance with the shared responsibility model;
* Ensure that CSP staff can only use the Database after they have completed training; and
* Ensure that your Organisation has contractual rights to directly monitor and audit the CSP's access and use of the Database.
 |
| Operational phase | * Implement periodic file reviews to assess whether files are being properly maintained in accordance with the shared responsibility model.
 |

**Risk 3: CSP staff access the Database for unauthorised purposes, or contrary to government-specific Database policies and procedures**

***Description of risk***

CSP staff may use the Database for unauthorised purposes, or access the database beyond what is needed to perform claims processing. For example, looking up a friend, relative, or celebrity for personal reasons, or copying parts of the Database to create their own version of the client's service record for convenience. In serious cases, CSP staff may illegally access or amend records for profit or other ulterior motives.

CSPs and their staff may not be familiar with Victorian government requirements like protective markings, statutory secrecy provisions, and retention / disposal requirements for public records.

Your Organisation must ensure the CSP and its staff clearly understand the scope and limits of access, and have mechanisms to regularly audit and verify appropriate Database use in practice. In past matters, staff have been unaware of what constitutes unauthorised access (and that unauthorised access is unlawful). It is also helpful to formally document the working arrangements between your Organisation and the portfolio agency, so that these requirements can be flowed down to the CSP.

(*Key PDP Act references: IPP 1.1, 2.1 and 4.1; VPDSS 2, 3, 4, 5 and 10*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Use technical configurations on databases to ensure that the CSP only has access to the relevant information in the client record (e.g. on a "need-to-know" basis);
* Consider if the Database can log access of the Database by individual users, and whether the Database should include this functionality;
* Develop a written services description / workflow document that explains how the CSP staff should use the Database;
* Consider appropriate on-boarding training program for CSP staff and who is responsible to conduct this training; and
* Consider if Database users should undergo security clearances / background checks.
 |
| Contract terms | * The CSP should commit to an agreed services description / workflow document, and ensure that its staff only access the Database for the purpose of providing the Services (and for no other purposes);
* Specify the level of access and whether the CSP can extract / edit information;
* Ensure that CSP staff can only use the Database once they you have approved them after being satisfied that they completed relevant training and security checks;
* Require the CSP to notify your Organisation of any suspected or confirmed misuse of the Database by its staff. The Contract could specify a timeframe to notify, make serious misuse a contract default, or impose abatements for breaches; and
* Ensure your Organisation has contractual rights to directly monitor and audit the CSP's access and use of the Database.
 |
| Operational phase | * Your Organisation, CSP, or an external auditor should periodically (annually or biennially) audit the CSP's access to the Database to identify any instances of unauthorised use;
* Ensure and review technological configurations and restrictions identified during the pre-contract stage (e.g. disable printing functionality);
* Consider how the CSP will be notified of policy updates / new policies during the term of the outsourcing arrangement; and
* If the Database administrator maintains a register of third party CSPs with access to the Database, ensure that the CSP is added to that list.
 |

**Risk 4: Ownership and control of the client files may not be clearly defined or understood**

***Description of risk***

Although the day-to-day responsibility for managing the Database will be shared, it is important to make clear that your Organisation retains overall ownership and control of the client files.

(*Key PDP Act references: IPP 1, 2.1, 3, 4.2, 5 and 6 ; VPDSS 1, 2, 3, 7 and 8.*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Liaise with your Organisation's information and records management team to ensure that:
	+ appropriate data retention and archiving procedures (in accordance with your Organisation's requirements) are implemented from the outset;
	+ the Case Management System and shared client files are added to your Organisation's information asset and risk management registers;
	+ appropriate information governance roles for the Case Management System are allocated within your Organisation, so that there are clear lines of accountability for governance of the Case Management System; and
* Consider developing policies and procedures that set out how your operations team will work with CSPs to manage issues such as information access requests and privacy complaints.
 |
| Contract terms | * The contract should clarify that the CSP is handling the client files only for the purpose of providing the services. While it is preferable that use of the Database be governed by the contract, if there are other necessary agreements, instructions or procedures, make sure they are consistent with the contract;
* The CSP should be required to return all copies of the client files to your Organisation at the end of the contract term; and
* The CSP should be required to comply with any relevant policies or procedures developed during the pre-contract phase (such as archiving and the relevant retention period for information).
 |
| Operational phase | * Ensure that the recommendations from your information and records management team are implemented;
* Consider how the CSP will be notified of policy updates / new policies during the term of the outsourcing arrangement;
* Prepare a list of the key information governance contacts for the Case Management System within your Organisation, so that this information is available for other members of your team and your successor; and
* The CSP should also consult with your operations team on information access requests, privacy complaints and document lifecycle issues.
 |

**Risk 5: Insufficient Identity Access Management planning and controls**

***Description of risk***

Your Organisation should be notified of CSP staff with access to the Database, and for what purposes. This will assist your Organisation to appropriately monitor their usage of the Database, and identify any cases of suspected or actual misuse. CSP staff should have their access to the Database promptly revoked once they no longer require access. For example, because they leave the CSP or change jobs within the CSP.

Identity and Access Management (**IDAM**) refers to the combination of policies, procedures and technical measures implemented to achieve these objectives. To be effective, IDAM requires continued management during the life of the outsourcing arrangement. IDAM problems can arise where the CSP does not promptly notify your Organisation about staff turnover / role changes, or where your Organisation does not conduct regular audits to supervise use of the Database by CSP staff.

(*Key PDP Act references: IPP 4.1, VPDSS 4, 5 and 10.*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Work with technical and operational stakeholders to ensure that a suitable IDAM strategy is implemented to manage the CSP's access.
 |
| Contract terms | * The CSP must notify your Organisation of CSP personnel with access to the Database, and promptly notify your Organisation of any changes in its user base;
* The CSP should ensure that its staff do not share their access credentials; and
* If the Database has an IDAM policy and procedures document, consider including this in the contract.
 |
| Operational phase | * Promptly remove access to CSP users who no longer require access; and
* Conduct periodic reviews of the authorised user list (for example, every three months) to confirm that it remains accurate and up to date.
 |

**Risk 6: Service delivery may be disrupted if the Case Management System is unavailable**

***Description of risk***

Once the Case Management System has been implemented, your operations team and the CSP will be relying on it to perform your functions and deliver the services to the public. Your operations team should consider how you would manage a situation where the Case Management System becomes unavailable for an extended period of time (for example, due to a severe technical outage).

The VPDSS requires your Organisation to implement appropriate business continuity and disaster recovery planning (**BC/DRP**) arrangements to ensure that the client files are available and accessible when they are needed by your Organisation and the CSP.

These BC/DRP arrangements are likely to include certain technical safeguards (such as data backups and secondary disaster recovery sites), which will be arranged by your technology services team. However, you should discuss this issue with your technology services team to understand what level of coverage is provided. You should then consider what manual work-arounds you could implement in the event that these technical measures are not able to bring the Case Management System back online within a reasonable period of time.

(*Key PDP Act references: IPP 3 and 4.1, VPDSS 2, 3 and 7.*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Liaise with your technology services team to understand what technical measures are being implemented to ensure business continuity; and
* Consider what manual work-arounds you could implement if the Case Management System is unavailable for an extended period. Document these work-arounds in a business continuity plan for your operations team.
 |
| Contract terms | * The CSP should comply with your Organisation's policies and procedures for the Case Management System, including the business continuity plan.
 |
| Operational phase | * Before the Case Management System goes live, undertake testing to ensure that it is operating correctly and performing to the required level;
* Once the Case Management System goes live, consider having a transition period where your operations team and the CSP maintain parallel copies of the client files outside of the Case Management System until the Case Management System has proven that it can safely operate at a full "business as usual" capacity; and
* Discuss the business continuity plan with the CSP, so that they understand how outages in the Case Management System will be handled.
 |

**Risk 7: Insufficient oversight and auditing of CSP usage of the Database**

***Description of risk***

It is important for your Organisation oversee the CSP during the contract. The security controls, training and documentation that are implemented at the start of the arrangement may need to be updated due to staff turnover, operational changes, or the emergence of new types of security threats. Regular audits are important to ensure CSPs actively manage their responsibilities under the contract.

(*Key PDP Act references: IPP 4.1, VPDSS 2, 3, 4 and 5.*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Configure the Database to maintain audit logs of individual users' access to the Database, and to produce reports flagging any unusual usage patterns\; and
* Develop a plan to conduct periodic audits of the CSP's use of the Database.
 |
| Contract terms | * The CSP must co-operate with, and participate in, the audit process and promptly address any issues identified through the audit;
* Ensure that privacy and data security issues are added as agenda items for any governance forums / performance review meetings with the CSP;
* Consider a term that the CSP should provide an annual attestation of its compliance with privacy and data security obligations; and
* The CSP should nominate a suitably qualified authorised representative to liaise with your Organisation on privacy and data security issues.
 |
| Operational phase | * As part of handover to operations, ensure that contract managers and other relevant stakeholders are made aware of the audit mechanisms in the contract and the schedule for conducting audits;
* Ensure that the outsourcing arrangement is noted in any relevant risk registers maintained by your Organisation or the Database administrator; and
* During the term of the outsourcing, conduct regular audits of the CSP's usage of the database and discuss the results with the CSP.
 |

**Risk 8: CSP login details / access credentials compromised by a third party**

***Description of risk***

Your Organisation may have less visibility of whether CSP staff are handling their access credentials (such as log-in details and passwords) securely. Data breaches can occur where a CSP's access credentials are compromised by a malicious third party and used to gain unauthorised access to a database. Technical and operational security controls can be implemented to minimise this risk and mitigate the potential damage of any data breach.

(*Key PDP Act references: IPP 4.1, VPDSS 6, 9 and 11.*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Consider what parts of the client service record the CSP requires and whether current technical configurations can restrict CSP access, or if changes are needed;
* Consider how the CSP would access the Database, and liaise with the Database administrator about ICT security settings for third party access (e.g. multi-factor authentication, Transport Layer Security, or Virtual Private Networks access); and
* Consider any minimum technical security requirements for the CSP's IT systems and whether the CSP complies with relevant industry standards in information security (e.g. ISO 27001).
 |
| Contract terms | * The CSP should comply with the minimum technical security requirements for the CSP's IT systems (if any), or any industry standards that it claims to be compliant with; and
* The CSP should immediately notify your Organisation of any actual or suspected data breach, or compromise of the CSP's passwords or log-in credentials (including any data breach that affects the CSP's systems).
 |
| Operational phase | * Ensure that the outsourcing arrangement is noted in any relevant risk registers maintained by your Organisation or the Database administrator.
 |

Conclusion

The strategies above are intended to provide a starting point for privacy and data security planning, and are not exhaustive.

Privacy and data security controls should be considered on a case-by-case basis to ensure that the outsourcing arrangement meets the following general objectives for privacy and data security compliance:

**Objectives - Privacy compliance**

* The CSPs agree (and have the necessary know-how and operational capacity) to perform their role in managing the client files (and accessing the Case Management System) in a manner that is consistent with the requirements of the IPPs. For example, the IPP 4.2 requirement to avoid retaining copies of client personal information for longer than is needed, or the IPP 2 requirement to only use or disclose the client information for the purposes for which it was collected (or other purposes specifically permitted under IPP 2).
* The outsourcing arrangement is implemented in a way that addresses your Organisation's continuing IPP responsibilities in relation to the Case Management System. For example, the IPP 3 requirement to take reasonable steps to ensure that the client files are accurate, complete and up-to-date, or the IPP 4 requirement to take reasonable steps to protect the Database from unauthorised access and misuse.

For further information, see Step 4 - IPP planning and due diligence in the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*.

Your Organisation should also conduct a Privacy Impact Assessment, which provides a structured process for systematically considering and addressing the requirements of the IPPs.

**Objectives - Data security compliance**

* The CSPs agree (and have the necessary know-how and operational capacity) to perform their role in managing the client files (and accessing the Case Management System) in a manner that complies with the requirements of the VPDSS.
* Your Organisation has addressed the requirements of VPDSS 8 (Third Party Arrangements), including:
	+ the service agreement adequately explains how the CSP will manage risks across all four security areas (ICT, personnel, information and physical security) - see VPDSS 8 element E8.020;
	+ your Organisation has identified and assigned relevant information security roles and responsibilities to the CSP under the CSP contract - see VPDSS 8 element E8.040; and
	+ your Organisation has arranged to regularly monitor, review and validate the CSP's compliance with the terms of its access to the Database - see VPDSS 8 element E8.060; and
	+ your Organisation has arranged appropriate "wrap up" / disengagement arrangements upon completion or termination of the CSP's engagement - see VPDSS 8 element E8.090.
* The outsourcing arrangement is implemented in a way that addresses your Organisation's on-going VPDSS responsibilities in relation to the Case Management System - for example:
	+ the VPDSS 2 requirement to use consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability;
	+ the VPDSS 4 requirement to implement a structured process for controlling access to public sector information (including by external users, such as CSP personnel); and
	+ the VPDSS 9 requirement to notify OVIC of any data breach affecting information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET (or any other information with a BIL of level 2 ("Limited") or higher).

For further information, see "Step 3 - VPDSF planning and due diligence" in the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*.

Further Information

**Contact Us**

**t:** 1300 00 6842
**e:** enquiries@ovic.vic.gov.au
**w:** ovic.vic.gov.au**Disclaimer**

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Privacy and Data Protection Act 2014, or any other legal requirement, to individual cases.