

Privacy Act 1988

**Contractor Privacy Collection Statement**

**Rehabilitation Program and Veterans' Vocational Rehabilitation Scheme (VVRS).**

This collection statement outlines how we {insert service provider}, trading as [entity name], as a Contractor for the Department of Veterans' Affairs ('DVA', 'the department'), collects and handles your personal information in compliance with the *Privacy Act 1988*.

By providing your personal information to us, including information about your health, you consent to our collecting and handling of your personal information in accordance with this privacy collection notice to enable the delivery of the Rehabilitation Program or Veterans' Vocational Rehabilitation Scheme (VVRS).

The provision of services by the Department of Veterans' Affairs (DVA) under the Rehabilitation Program and VVRS is known as **Rehabilitation Services**.

Rehabilitation services are provided and administered by the department under DVA's legislation: the *Veterans' Entitlements Act 1986* (VEA), the *Safety, Rehabilitation and Compensation (Defence-related Claims) Act 1988* (DRCA), and the *Military Rehabilitation Compensation Act 2004* (MRCA).

The **Rehabilitation Program** is designed to help eligible Veterans to restore function, or achieve the highest possible level of function, physically, psychologically, socially, vocationally and economically; to maximise quality of life and wellbeing, and to minimise the person's long term health care needs and community support needs that have arisen as a result of their service.

The **VVRS** is designed to help eligible Veterans find or retain employment. The Scheme also offers Medical Management and Psychosocial Rehabilitation services to address barriers in other parts of the Veteran's life preventing their retention of, or return to, employment.

**Who is collecting your personal information?**

Your personal information is being collected by the [insert service provider], trading as [entity name] (ABN [insert ABN/ACN]) ('Us', 'We', 'Our') as a Contractor to DVA providing Rehabilitation Services.

**What personal information is being collected?**

We collect information about your service in the Australian Defence Force, your transition to civilian life and your current circumstances. This can include sensitive information, which is a category of personal information. This includes:

- Your name, date of birth, mobile number, email address and postal address
- Your service in the ADF including details around your discharge from service
- Your medical and other health information and details about your support needs
- Any other information pertaining to your need for Rehabilitation Services

**Why is your personal information being collected?**

The primary purpose for the collection of the information is to enable the provision of rehabilitation services to you on behalf of the department.

The secondary purpose for the information is to provide reports to the department on the rehabilitation services being delivered based on specific client needs as necessary for the department to administer the Rehabilitation Program.

**Who will we disclose your personal information to?**

We will share your personal and health information with:

- The department
- Your treating doctors, hospitals, and/or health professionals as required to facilitate your rehabilitation goals.
- Other support and service providers where necessary for the effective provision of your services
- Other parties where the release is authorised by law, including for the purpose of research or investigation.

We will not disclose your personal information outside of the above, unless it is authorised by law or we otherwise have your consent to disclose it.

#### **How will we manage your personal information?**

We will store your personal information securely and where it needs to be shared with the department and/or other service providers, to assist in the delivery of services to you, we will ensure that they have adequate information security measures in place to store and manage that information.

#### **What will happen if we don't collect your personal information?**

If you do not consent, this will affect our ability to deliver Rehabilitation Services to you under the VVRS and/or the Rehabilitation Program.

#### **Our Privacy Policy**

You can find out more about accessing and/or correcting your personal information with us, making a complaint and about our approach to managing personal information via our privacy policy which you can find at [link to Contractor's privacy policy]. For information about our privacy policy, please contact [Contractor's contact person].

If you have any questions about the collection of your personal information in accordance with this privacy collection notice, please contact [Contractor's privacy contact person].

Information regarding the privacy policy of the department is found here: [www.dva.gov.au/privacypolicy](http://www.dva.gov.au/privacypolicy)



**Australian Government**

**Department of Veterans' Affairs**

# **Privacy Management Plan Template**

**Name of Organisation:**     **(Insert Contractor Name here)**

## Glossary

APPs	Australian Privacy Principles. There are 13 APPs under the Privacy Act
APS Privacy Governance Code	Privacy (Australian Public Service – Governance) APP code 2018 to be implemented by the OAIC
Client	A DVA rehabilitation client who is commencing, or is on, a rehabilitation plan
Contractor	A DVA contracted organisation which provides services to rehabilitation clients
DVA	Department of Veterans' Affairs
Healthcare information	<p>This includes:</p> <ul style="list-style-type: none"> <li>• information collected in connection with the provision of a health service;</li> <li>• information or opinion about the health or disability of an individual;</li> <li>• an individual's expressed wishes about the provision of health services; and/or</li> <li>• information about health services provided to an individual.</li> </ul>
OAIC	Office of the Australian Information Commissioner
Personal information	As defined by the Privacy Act, this is information or an opinion about an identified individual, or an individual who is reasonably identifiable
Personnel	Employees of the Contractor
Privacy Act	<i>Privacy Act 1988</i>
PMP	Privacy Management Plan.
Sensitive information	As defined by the Privacy Act, this is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record that is also personal information, or health information or, genetic information about an individual, or certain biometric information.
the Policy	Privacy Policy.

## Introduction

The Department of Veterans' Affairs (DVA) is committed to the protection of personal information in a manner consistent with the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs).

DVA is also committed under the Rehabilitation Program to ensuring that sensitive and healthcare information accessed for the purpose of developing and executing a rehabilitation plan is managed in a manner that is consistent with the APPs and the state and territory privacy laws and healthcare regulation.

## General Expectations for Privacy Issues

### **For all types of information:**

When the Contractor or its personnel collect information, DVA requires that you:

- Obtain appropriate client consent for its collection and sharing through the completion of the Privacy Collection Notice template;
- obtain written confirmation from the client showing that the client has read and understood the Privacy Collection Notice;
- inform the client the purpose for collecting the information;
- inform the client where there is a mandated reason to seek the information eg: obtaining a medical certificate for incapacity purposes;
- explain how the information will be used;
- explain how the information will be stored;
- ensure information is shared in accordance with privacy requirements. Ie. Client privacy markers, on secure organisation email, etc.
- notify DVA in writing within one business day if you believe a client's privacy has been breached by your organisation; and
- ensure that Personnel within your organisation are respectful of client's privacy and that personal information is not unnecessarily shared within the organisation.

The following should be taken into consideration for various types of information:

### **Personal information**

Rehabilitation Contractors (Contractors) should only collect personal information where the information is reasonably necessary for, or directly related to the client's rehabilitation plan.

### **Healthcare information**

Contractors will ensure client consent is obtained at all times when accessing healthcare information. Consent is required to be reobtained every 12 months.

### **Other community organisation information**

Contractors will ensure that it is clinically necessary to obtain information from general community organisations. Client consent is required to be reobtained every 12 months.

## Privacy Management Plan for Rehabilitation

The Privacy Management Plan (PMP) is designed to ensure that Contractors meet their obligations under the requirements of the Privacy Act, the APPs and the DVA Deed for rehabilitation services. The requirement for a PMP is referenced in the Contract Management Provider Procedural Guideline.

Contractors have access to sensitive information about clients and their families. This includes substantial material on their accepted and non-accepted conditions, the status of their treatment plans and their general life circumstances. It is imperative that Contractors maintain exceptional privacy management controls within their organisation to ensure that all material and interactions with clients is kept in the strictest of confidence.

This plan is designed to assist Contractors to ensure that the privacy controls they have within their organisation is adequate and complies with DVA requirements.

The Contractor must update the PMP and resubmit a copy to DVA for approval annually in line with every one (1) year anniversary of Deed execution date, or within two (2) weeks of any relevant change in privacy law or best practice; or receipt of any comments from DVA.

## Instructions for the completion of the PMP Template

The PMP template is at Appendix 1. Contractors are required to complete all fields in columns 2, 3 and 4 as described.

The PMP is required for all organisations, regardless of its size.

The PMP is due on every one (1) year anniversary of the Deed execution date.

## Resources

Other resources relevant to this document include the following:

- The Deed for Rehabilitation Services.
- Privacy Act ([www.comlaw.gov.au](http://www.comlaw.gov.au))
- Office of the Australian Information Commissioner ([www.oaic.gov.au](http://www.oaic.gov.au))

## Appendix 1 – Privacy Management Plan Template

**Contractor Name:** *Add Organisation Name Here*  
**Plan Date:** DD Month 202X to DD Month 202X

Area 1 - Embed a culture of privacy that enables compliance			
DVA Requirement	Position within organisation responsible for this requirement	Outline how the organisation will comply with this requirement	Evidence to support this/these claim(s), and include attachments
The organisation has assigned a member of their personnel who is responsible for managing privacy issues for DVA clients in your organisation.			
Reporting mechanisms that ensure senior management are routinely informed about privacy issues have been created and are in place.			
Personnel understand their privacy obligations and integrate privacy into staff training and induction and keep them up to date.			
An organisational privacy policy has been developed, implemented, which includes developing and maintaining processes around the handling of personal information prior to collection, while personal information is held and once the plan has closed.			



DVA is notified in writing within one business day if a privacy breach has occurred and consulted prior to any notification of clients or OAIC or other authority under the Privacy Act, eligible data breach provisions.				
Area 2 – Collection, Usage and Integrity of Personal Information				
DVA Requirement	Position within organisation responsible for this requirement	Outline how the organisation will comply with this requirement	Evidence to support this/these claim(s), and include attachments	
Informed client consent is obtained at all times and that it is clearly explained to the client why the information is required and how it will be used and disclosed. This is especially important for healthcare information.				
Personal information is not collected unless the information is reasonably necessary for, or directly related to the development or execution of a rehabilitation plan.				
Personal information that is collected, used or disclosed is accurate, current, complete and relevant.				
Personal information is protected from misuse, interference, loss and from unauthorised access, modification or disclosure.				



Information is shared in accordance with privacy requirements. i.e. Client privacy markers, on secure organisation email, etc.			
Clients have access to their personal information at all times, and that there is systems in place so that clients know they can do this.			

Area 3 Storage of Personal Information			
DVA Requirement	Position within organisation responsible for this requirement	Outline how the organisation will comply with this requirement	Evidence to support this/these claim(s), and include attachments
Risk management processes have been implemented to identify, assess and manage privacy risks associated with IT security breaches.			
Personal information is stored correctly i.e. client information is locked and secured when not in use and protected from unauthorised access. Encryption is used where sensitive information is stored and in transmission.			
The Contractor may use a cloud based ICT system to store personal information collected on behalf of the Department in the delivery of services under this Deed provided that their ICT system:			

<p>a) is capable of certification in accordance with the Whole of Government Hosting Certification Framework, Information Security Manual, Protective Security Policy Framework; and</p> <p>b) does not permit the offshore transfer of personal information collected on behalf of the Department.</p> <p>c) Privileged accounts and technical support is conducted and held within Australia</p> <p>Cloud based services must be conducted in accordance with the Australian Government Secure Cloud Strategy.</p> <p>All solutions including the required integrations are to be developed and configured to meet and support Australian Government security standards including, but not limited to:</p> <ul style="list-style-type: none"> <li>• Australian Government Protective Security Policy Framework (PSPF),</li> <li>• Australian Government Information Security Manual (ISM),</li> <li>• Australian Signals Directorate (ASD) Essential Eight,</li> <li>• ISO27001 - Information Security Management,</li> </ul>		
---	--	--

- |   |  |  |  |
|---|--|--|--|
| <ul style="list-style-type: none"><li>• Digital Transformation Agency (DTA) Whole-of-Government Hosting Strategy,</li><li>• Australian Privacy Act 1988 and Australian Privacy Principles (APPs).</li></ul> |  |  |  |
|---|--|--|--|

SIGNATORIES:

Contractor Signature: \_\_\_\_\_

DVA Contract Manager Signature: \_\_\_\_\_

Contractor Name: \_\_\_\_\_

DVA Contract Manager Name: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_