

PRIVACY COMMITMENT

We understand that your privacy is important to you and we are committed to handling your personal and health information responsibly in compliance with the *Privacy Act 1988 (Cth)*, the Australian Privacy Principles, the *Aged Care Quality Standards*, the *NDIS Practice Standards* and the *National Principles for Child Safe Organisations*.

This policy outlines how BCR Communities meets our obligations and how we handle the personal and sensitive information which you (or your parent, guardian, carer or other support person) provides to us so we can provide you with supports and services.

By applying for or using any of the supports or services we provide and/or by providing us with your personal information, you agree to your personal information being collected, held, used and disclosed as set out in this Privacy Policy.

INFORMATION WE COLLECT

The type of information we collect about you depends on the nature of your relationship with BCR Communities – whether for example you are a client, participant, job applicant, contractor, volunteer or staff member.

This information may include:

- Identifying and contact information such as name, date of birth, address, telephone number, email address
- Government identifiers such as Medicare number, My Aged Care ID, Tax File number
- Financial information, such as banking, payment and contribution details
- Health information required to provide you with the supports and services you seek
- Information to deliver culturally appropriate services, such as religious, racial and ethnic background including if you identify as an Aboriginal and Torres Strait Islander person

Following the definitions in the *Privacy Act 1988*;

- **Personal information** is information about you that also identifies you.
- **Sensitive information** is information about you such as health, disability, ethnic origin, beliefs or sexual orientation.

USE AND DISCLOSURE OF YOUR PERSONAL INFORMATION

We only collect personal information (including sensitive information) to provide you with supports and services (including third party products and services) you've applied for, to identify you, to manage your account and improve the services you receive.

Whenever it is reasonable and practicable to do so, we will collect your personal information directly from you. If we are unable to collect information directly from you, we may also collect information from third parties to manage your supports and services and to better understand you, your preferences and interests.

We also use this information to comply with our legal obligations.

Some uses include:

- Identify you
- Provide and manage a product or service, including assisting you to complete online applications, answering your enquiries and complaints
- Plan and deliver your supports and services
- Help us to improve the delivery of supports and services, enhance our relationship with you and to effectively manage risks
- Enabling contact with a nominated person, General Practitioner or other health professionals involved in your care
- Understand your interests and preferences so we can tailor our products, services and marketing to tell you about other products and services that may be of interest to you
- Manage our rights and obligations regarding external payment systems, including claiming and receiving funding due to us in advance or in arrears for services planned or provided to you
- Assess an application for employment or volunteering with us
- Processing of wages
- Interact with regulators and government departments or agencies in relation to a complaint made by you or your representative, or an incident that is reportable to a regulator under an Act or regulation, and
- Comply with legal or regulatory obligations imposed on us.

BCR Communities may disclose your personal information to our Employees, Volunteers and registered Third Party Providers when you consent to receive supports or services from them. We only disclose the personal information required to fulfil these services. All Employees, Volunteers and registered Third Party Providers are vetted, verified and bound to respect the privacy of your personal information.

If you choose not to provide us with some or all of the information we request, we may not be able to provide you with the supports and services you require.

HOW WE USE YOUR INFORMATION TO TELL YOU ABOUT OUR SUPPORTS AND SERVICES

We may use your personal information to tell you about the supports or services you have requested or that we think might benefit you via:

- Email
- SMS, or other electronic notification
- Social media and other digital platforms
- Our website or apps
- Mail, or
- telephone

You can contact us at any time to 'opt out' of receiving these communications by calling us on 1300 222 748.

STORAGE AND SECURITY OF YOUR PERSONAL INFORMATION

BCR Communities takes reasonable steps to ensure that the personal or health information it collects and holds is protected from misuse, interference, loss, unauthorised access, modification or disclosure.

Personal and health information kept by BCR Communities in printed form is stored in secure premises. In electronic form, it is held in secure storage systems requiring login details and passwords. Access to personal or health information is limited to those who specifically require it to conduct their responsibilities.

Our employees, volunteers and contractors are bound by a Code of Conduct to maintain the confidentiality of your personal information. Third Party Providers are bound by a Brokerage Agreement to maintain the confidentiality of your personal information. All employees and volunteers of BCR Communities undertakes privacy training so that they know how to keep your information safe and secure. Other parties are bound by Confidentiality Agreements.

ACCESSING AND CORRECTING PERSONAL INFORMATION WE HOLD ABOUT YOU

We take reasonable steps to ensure that the information we hold about you is accurate, complete and up-to-date. To assist us with this, please provide us with correct information and inform us if your details change.

You have the right to access your personal information and request any corrections. Please contact us if you wish to view and/or correct personal or health information we hold about you. For security reasons, a written request may be required to access your health information. We are committed to granting you access to your personal information within a reasonable time frame. We will not refuse you access unless there are legal reasons for doing so. In such circumstances, we will explain those reasons to you.

If you have any questions about how we deal with personal information, wish to complain about a breach (or suspected breach) of your privacy, or correct your personal information, please contact our Privacy Officer on info@BCRcommunities.com or 1300 222 748.

If the matter is not resolved to your satisfaction, you can contact:

Office of Australian Information Commission (OIAIC)
GPO Box 5288,
Sydney NSW 2001
Phone: 1300 363 992.
Email: foi@oaic.gov.au
Website www.oaic.gov.au

PROTECTING YOUR PERSONAL INFORMATION

BCR Communities is committed to keeping secure the Personal and Sensitive information you provide to us. We will take all reasonable steps to ensure the information we hold is protected from misuse, interference, loss, from unauthorised access, modification or disclosure.

We hold your personal information in a combination of hard copy and in electronic form. Some of your information is in secure data centres that are located in Australia and some with selected service providers, including cloud service providers.

Our information technology systems ensure we can meet the needs of BCR Communities, ensure the protection of consumer, staff and organisation information and support the collection of service delivery data and reporting obligations outlined in our Funding and Grant Agreements.

We hold your personal information for as long as it is required to provide you with supports or services, or for any period we are required to keep that information by law. If we no longer require your personal information for any purpose, we will take reasonable steps to securely destroy or permanently de-identify that information in accordance with destruction and retention requirements.

BCR employees and volunteers shall NOT make any statement to the press, radio or television station or to any reporter for the media. If a BCR staff member is approached to make a statement or comment, they are to refer the person to the BCR Chief Executive Officer.

CYBER SECURITY

Strategies adopted by BCR Communities to ensure the safety of data include:

- All data is synchronised to the cloud. We only utilise cloud storage physically based in Australia (data sovereignty) and only accessible within BCR's private network.
- We utilise a Unified Threat Management firewall (UTM)
- All computers are password protected. We employ a user access policy where users are only granted access to data that they require to do their job
- Service delivery staff only have access to the data of clients they are working with or likely to work with. Access is limited to information directly related to their work such as the support plan and notes.
- Mobile device manager (MDM) software is utilised to manage all access to data by Home Care Workers and other staff using mobile phones. This includes remote wipe and remote delete functions for use in the event of loss of the device.

ELIGIBLE DATA BREACH

Not all data breaches are required to be notified to the Information Commissioner and affected individuals. The new notification requirements relate only to an Eligible Data Breach (a concept as defined in the legislation). Eligible Data Breach is a data breach involving personal information that is likely to result in Serious Harm to any individual who the information relates to.

Serious Harm where harm is “more probable than not” having regard to a number of factors listed in the Notifiable Data Breaches Act including (not an exhaustive list):

- a) the kind of information;
- b) the sensitivity of the information;
- c) how the information is protected;
- d) who the persons are who could have obtained the information; and
- e) the nature of the harm.

Serious harm can include:

- a) serious physical harm
- b) psychological harm
- c) emotional harm
- d) economic harm
- e) financial harm
- f) serious harm to reputation; and
- g) other forms of serious harm that a reasonable person in the organisation’s position would identify as a possible outcome of the data breach.

Although individuals may be distressed or otherwise upset that a data breach has occurred, this is not of itself sufficient to trigger the requirement to notify unless a reasonable person in the organisation’s position would consider that the likely consequences for those individuals would constitute a form of Serious Harm.

WHAT HAPPENS IF THERE IS A DATA BREACH

In the event of any loss, or unauthorised access or disclosure of your personal information that is likely to result in serious harm to you, we will investigate and notify the Office of the Australian Information Commission (OAIC) and other relevant regulatory bodies, and notify you as required under Privacy Laws.

The following process would be implemented:

- Step 1** Contain the breach, make a preliminary assessment and designate person/team to coordinate response; BCR’s Chief Executive Officer and Executive Managers will be notified of suspected data breach
- Step 2:** Assess and evaluate the risks for individuals and BCR Communities - the parties associated with the breach. Consider whether the data breach is an Eligible Data Breach and whether a breach notification is required. Establish the cause and extent of the breach and identify the risk of harm.
- Step 3:** Consider breach notifications. If the breach or suspected breach may result in serious harm to an individual or BCR Communities, BCR Directors and relevant government bodies will be informed. It is important to note that not all breaches necessarily warrant notification.
- Step 4** Take action to prevent future breaches. Fully investigate the cause of the breach and consider developing a prevention plan. Make appropriate changes to policies and procedures. Revise all staff training practices

BCR’s Data Breach Response Plan provides guidance on how to action each of the above steps.

NOTIFYING THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSION (OAIC)

Once BCR Communities has reasonable grounds to believe an Eligible Data Breach has occurred we will provide a statement to the OAIC as soon as practicable after we become aware of the eligible data breach.

We will advise the OAIC if we believe that another entity regulated by the Notifiable Data Breaches Act is involved in the eligible data breach.

ENTITIES COVERED BY THIS POLICY

BCR Communities is a community led, not-for-profit organisation servicing the Shoalhaven and Illawarra. We have a team of dedicated staff and volunteers who support our communities through our quality Aged Care, NDIS and Community Services including our Community Radio Station – Bay & Basin 92.7FM

These subsidiaries are subject to the same standards for handling of personal information, regardless of which service they provide.