BLUE MOUNTAINS WOMEN'S
HEALTH & RESOURCE CENTRE
ABN: 18334739140
reception@bmwhrc.org
(02) 4782 5133

*At Blue Mountains Women's Health & Resource Centre we acknowledge the Traditional Owners of the land on which we live and work, and we celebrate diversity in all its forms.*

Blue Mountains Women's Health & Resource Centre Inc.

# Privacy & Confidentiality Policy

| | |
|---|---|
| Relevant legislation | Health Records and Information Privacy Act 2002 (NSW); Safe Work Australia, Managing Psychosocial Hazards at Work, Code of Practice; Privacy Act 1988 (Cth); Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth); Privacy and Personal Information Act 1988; Privacy Amendment (Enhancing Privacy Protection) Act 2012; Children and Young Persons (Care and Protection) Act 1998; Fair Work Act 2009 (Cth) |
| Standards or other external requirements | RACGP; National Principles for Child Safe Organisations; NBMLHD; DCJ; DSS. |

## Introduction

BMWHRC is committed to protecting and upholding the right to privacy of service users, staff, students, volunteers, Management Committee members, and representatives of agencies we deal with. BMWHRC is also committed to protecting and upholding the rights of our service users to privacy in the way we collect, store and use information about them, their needs, and the services we provide to them.

## Purpose

This policy outlines BMWHRC's position privacy, health information, consent, and issues relating to the use of information.

## Definitions

***Privacy*** is defined in federal law and relates to personal information, including names, addresses, phone numbers, other identifying information, and health-related information.

***Confidentiality*** is defined under common law, and relates to protections of personal information over and above the legislative requirements, often defined in organisational confidentiality policies.

*Consent* is providing permission for data to be collected and used in specific instances. Informed consent is when the person providing the consent has sufficient information and capacity to understand the risks involved when providing consent.

*Capacity* is having a sufficient level of intellectual maturity to make decisions for oneself, in particular relating to whether or not to consent to have information collected and used.

*Personal information* is information which directly or indirectly identifies a person. This may include written documentation or may also include images and videos of a person.

*Health information* is a specific type of personal information that includes anything relating to a person's physical or mental health, or about similar health-related issues in a person's family history.

*Privacy breach* means any occasion, intentional or otherwise, where personal information collected by BMWHRC is made available to third parties or to the public without consent, whether that information is known to have been viewed or not.

*De-identified data* is data where identifying information, such as name and address, has been removed. The level of de-identification must be appropriate for the likelihood of being identified. For example, age, gender and racial background might be considered sufficiently identifying information in a small community. The purpose of de-identifying information is to be able to report on some data without risk of a privacy breach.

## Privacy

BMWHRC will meet its legal and ethical obligations as an employer and health service provider in relation to protecting the privacy of service users and personnel. BMWHRC is subject to *The Privacy Act 1988 (Cth)* and, as such, BMWHRC will follow the thirteen Australian Privacy Principles (see Appendix 1).BMWHRC follows the following principles as a minimum standard in relation to the collection and use of personal information:

- Collect only information which the organisation requires for its primary function. Do not collect information that is not required for BMWHRC to provide or review its services.
- Ensure that clients are informed about their rights regarding privacy and confidentiality, including why their information is collected and how we manage and maintain the information gathered. Where this information relates to children, information will be provided in a way that is appropriate for them and their guardian.
- Use and disclose personal information only for primary functions of the organisation or a directly related purpose, or for another purpose with the person's consent.

- Collect and store personal information securely, protecting it from unauthorised access; and
- Provide stakeholders with access to their own information, and the right to seek its correction.

## Health Information Privacy

Specific provisions exist in relation to health information under the *Health Information Privacy Act* 2002 (NSW). This legislation:

- Protects clients' privacy rights by ensuring health information is collected, stored, used or released using the Health Privacy Principles (HPPs). BMWHRC is committed to the HPPs (see Appendix 2).
- Allows for the right of clients to see and ask for changes to be made to personal health information.
- Allows clients to make complaints to the NSW Privacy Commissioner if health information has been misused or if the HPPs have been breached.

Under Chapter D of *the Privacy Act 1988 (Cth)*, APP3 and APP6of the 13 Privacy Principles (see Appendix 1) do not apply to BMWHRC when collecting health information. BWMHRC may collect, use and disclose personal information where doing so is required or authorised by Australian law and/or where to do so is required or authorised in accordance with rules established by a competent health or medical body that deals with professional confidentiality and which binds BMWHRC.

## Consent

When collecting and using information, consent must be given. BMWHRC follows the following principles in attaining consent:

- *The individual must have the capacity to provide their consent:* All adults should be assumed in the first instance to have capacity, regardless of their situation. Meeting capacity may require conveying information in different ways depending on an individual's circumstances. Capacity must include a sufficient understanding of any risk involved by providing consent.
- *The consent must be freely given:* No person will be, or will feel to be, coerced or pressured into giving consent.

reception@bmwhrc.org
(02) 4782 5133

- *The consent must be sufficiently specific for the purpose it is used:* Consent is only valid for the purpose it was given, and new consent must be attained if information is going to be used for new purposes or new information is being gathered.
- *The consent must be informed:* Providing information is not sufficient for making sure consent is informed. The individual must make it clear they understand what they are consenting to, and this may require discussion.
- *The consent must be current:* Attaining consent is an ongoing discussion, and participants may be required to re-affirm their consent over time to ensure it is current.

Consent for collecting and using information will be provided in writing. In some circumstances, verbal or implied consent may apply when a person's actions show their consent, but this will not be assumed in the collection, use, or disclosure of personal or health information.

Whenever attaining consent, staff will explain the principles of consent, and that consent can be withdrawn at any time. They must also explain the type of information to be collected, the purpose of that collection, how it will be used, who else will have access to it, and whether they are able to change the information. Conditions leading to mandatory reporting or disclosure must also be explained.

## Consent for children and young people

As far as possible, these principles will apply to children. Legislation does not provide a specific age of consent. The age and development of a child will determine their capacity to provide consent, but this must be determined on a case-by-case basis.

It is assumed that most children may provide informed consent over the age of 12, and where a child does have capacity, they may provide their own consent. Where a child does not have capacity, their legal guardian may provide consent on their behalf.

If a child has provided consent without the knowledge of their legal guardian, staff should explain the circumstances in which information may be disclosed to their guardian. Information should not be disclosed to their guardian except where the service is required to do so, or where the child's safety requires this information be shared.

In instances of mandatory reporting, it may be necessary to share information without the consent of the child. This should be explained to the child prior to the child providing their consent. See HR5.15 Child Safety.

reception@bmwhrc.org
(02) 4782 5133

## Collecting, using and storing information

BMWHRC staff collect, use, and store staff, client and community information when using BMWHRC's services. Copies of information will not be made, except when required for the purpose for which it was collected.

De-identified data may be used and disclosed to third parties for the purposes of reporting on BMWHRC's activities where it is required to do so by law or under contract.

Full provisions for the collection, use and storage of personal information is covered under OP8.5 Data management and breach.

## Information access

A service user or staff member may have access to their own information on request. This information may be updated or corrected by the person it relates to at any time. BMWHRC will ensure that this access is provided in a manner that is timely, private, and protects the safety of other clients. Where a current or former staff member has made a request for this information, BMWHRC must make it available within three days in person or 14 days via mail.

## Privacy complaints

BMWHRC is committed to transparency. Any client, community member, or member of the public may provide notice to BMWHRC if they believe any breach of privacy has been made by BMWHRC, whether intentionally or unintentionally. All complaints will be acted upon by BMWHRC staff and the Management Committee as a matter of urgency. Any complaints received regarding privacy breaches must be communicated to the Management Committee. An immediate assessment of any complaint must be made and, if a breach has been confirmed, confirmation of actions taken must be made to the complainant.

## Privacy breach

A privacy breach is the unintentional or unauthorised access, disclosure or loss of data. A notifiable breach is one that must be reported to the individual(s) affected and to the Office of the Australian Information Commissioner within 30 days of the breach. A data breach is considered notifiable if it involves personal information, if the breach may cause serious harm, and if remedial action cannot remove the risk of harm.

Full information regarding privacy breaches is covered under OP8.5 Data management and breach.

reception@bmwhrc.org
(02) 4782 5133

# Appendix 1 – Australian Privacy Principles

APP 1. Open and transparent management of personal information: Ensures that BMWHRC manages personal information in an open and transparent way.

APP 2. Anonymity and pseudonymity: BMWHRC provides the option for individuals not to identify themselves or use a pseudonym as far as possible, with limited exceptions.

APP 3. Collection of solicited personal information: BMWHRC will collect personal information within the guidelines of the Act when it is solicited.

APP 4. Dealing with unsolicited personal information: Ensures that BMWHRC attains permission before using unsolicited information, or else manages and/or destroys it.

APP 5. Notification of the collection of personal information: Ensures permission is attained to use information either prior to or as soon as practicable after information is collected.

APP 6. Use or disclosure of personal information: Information will only be used or disclosed for the primary purpose for which it has been collected, or a secondary purpose if consent is provided (unless required by law).

APP 7. Direct marketing: BMWHRC will not use information it collects for direct marketing purposes unless consent to do so has been provided.

APP 8. Cross-border disclosure of personal information: Where information is disclosed to third parties outside Australian legal jurisdictions, efforts must be made to ensure Australian privacy law and Privacy Principles are not breached by the third party.

APP 9. Adoption, use or disclosure of government-related identifiers: BMWHRC will not use or disclose government-related identifiers unless authorised by law.

APP 10. Quality of personal information: BMWHRC will ensure, to the best of its ability, personal information is accurate and maintained.

APP 11. Security of personal information: BMWHRC will maintain strict security measures when collecting, storing, handling, using or removing information.

APP 12. Access to personal information: BMWHRC only allows access to authorised personnel for the purpose of its primary purpose, or secondary purposes where consent has been given. BMWHRC also allows access to personal information for those to whom the information pertains.

APP 13. Correction of personal information: Individuals have the right to review and correct any personal information BMWHRC holds about them.

reception@bmwhrc.org
(02) 4782 5133

# Appendix 2 – Health Privacy Principles (HPPs)

As a health service, the following principles also apply to BMWHRC.

HPP 1. Lawful: BMWHRC only collects information for lawful purposes.

HPP 2. Relevant: The data collected by BMWHRC must be relevant to the primary and/or secondary purposes of its work.

HPP 3. Direct: Health information must be collected from the person themselves rather than through a third party (unless it is unreasonable or impractical to do so).

HPP 4. Open: BMWHRC is open about when and why it collects information and communicates this to its service users. It also provides information on the rights, access and other information relating to collection and use of health information.

HPP 5. Secure: BMWHRC stores information securely, only keeps this information for as long as necessary, and destroys information when it is no longer required. Only those who need access to this information have it.

HPP 6. Transparent: BMWHRC will provide information to service users about the information they have, why it is held, and their rights to access it.

HPP 7. Accessible: Service users at BMWHRC will have access to their own health information when they request it without unreasonable expense or delay.

HPP 8. Correct: Individuals can update the health information BMWHRC has of them on file.

HPP 9. Accurate: To the best of its knowledge, the data BMWHRC keeps is accurate. It updates data when it becomes aware of any changes to information and regularly maintains its data.

HPP 10.Limited Use: BMWHRC will only use health information for the purpose for which it was collected, or to a secondary purpose that is reasonable in the running of BMWHRC. Additional usage requires additional consent. In some legislated instances, this principle does not apply.

HPP 11. Limited Disclosure: BMWHRC will only disclose health information to third parties for the purposes for which it was collected, or a directly related purpose it would be reasonable to expect. Additional disclosure requires additional consent. In some legislated instances, this principle does not apply.

HPP 12.Non-identification: BMWHRC can only provide service users an identification number if it is reasonably necessary to carry out its functions.

HPP 13. Anonymity: Service users will have the option of receiving services anonymously, where lawful and practicable.

HPP 14. Controlled linkages: Information will only leave the jurisdiction of NSW if necessary.

HPP 15. Authorised linkages: Information will only leave the jurisdiction of NSW when consent has been provided.