Confidentiality and Privacy Policy

134-020

Version Number: 4.0

Approving Authority: Board of Directors

Date of Approval: September 2002

Review Dates: September 2005, November 2008, February 2012, April 2014

Date of Next Review: April 2017

Purpose:

The purpose of this policy is to ensure that sound systems are in place to ensure the privacy and confidentiality of client information and access to this information on request.

Scope:

This policy applies to all Board Directors, employees, volunteers, students and contractors at Banyule Community Health.

Policy Statement:

Banyule Community Health collects personal information and health information from individuals that are necessary to provide a safe and quality service. It uses this information to deliver health services to individuals, and for approved secondary purposes such as funding, management, planning, monitoring, improvement or evaluation, or training provided by the health service to employees or persons working with the organisation.

Banyule Community Health is committed to:

- Responsible handling of health information, and protecting the privacy of an individual's health information
- Upholding the right of individual's to access their health information, except where this may pose a serious threat to the life or health of the individual or another person
- Respecting the dignity and privacy of the individual, at all times

Banyule Community Health will at all times endeavour to ensure that information is not disclosed that would identify a person as receiving health services from BCH, without that persons consent, unless permitted or required under legislation. It will abide by both Australian Privacy Principles and Victorian Health Privacy Principles.

In order to meet these commitments, Banyule Community Health will:

- Only collect personal information from individuals where it is necessary for one or more of BCH functions or activities
- Collect this information by lawful and fair means, minimising intrusion as far as possible.
- Only use the health information of clients for the purpose for which it is intended or where the client has consented to the use or disclosure, or for a secondary purpose related to the primary purpose and which the client would reasonably expect it to be used
- Ensure as far as is practicable that all health information collected and held is maintained as accurate, complete, up to date and relevant to the purpose for which it was collected
- Take reasonable steps to correct information where information is found to be inaccurate, incomplete, or not up to date
- Maintain client health information in secure client information

management databases that protects the information from misuse, loss or unauthorised access
- Provide systems for individuals to access their own health records
- Communicate these systems to users of the health service
- Ensure all staff are provided with the Health Privacy Principles of the Health Records Act 2001 at orientation
- Ensure that all external auditors and contractors comply with Privacy Legislation and BCH Policy
- Provide training to staff in Privacy and Confidentiality as it relates to health records and personal information
- Act promptly to resolve any complaints regarding the handling of health information, and provide information on complaint resolution mechanisms
- Not disclose any personal information to overseas recipients.

Banyule Community Health does not collect sensitive information about its clients unless the client consents and the information is needed to provide a service to the client.

Banyule Community Health will appropriately manage any personal information received about an individual that was not sought by Banyule Community Health and not needed for the provision of services

This policy and its related procedure will be made available on request to clients of the health service without charge, and will be available on the home page of the Banyule Community Health website.

Definitions:

Health information is defined in section 3 of the *Health Records Act* 2001 as:

a) "information or opinion about –
   i. the physical, mental or psychological health (at any time) of an individual; or
   ii. a disability (at any time) of an individual; or
   iii. an individual's expressed wishes about the future provision of health services to him or her; or
   iv. a health service provided, or to be provided, to an individual –
   that is also personal information; or
b) other personal information collected to provide, or in providing, a health service, or
c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at

any time) of the individual or of any of his or her descendants –
but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information…"

Personal information is defined in section 3 of the Health Records Act 2001 as:
"information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded In a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years."

Sensitive information is defined in the Privacy Act 1988 as meaning 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 preferences or practices
- criminal record

that is also personal information or health information about an individual

- genetic information about an individual that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification
- biometric templates.

Employee record in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;

- the employee's membership of a professional or trade association;
- the employee's trade union membership;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- the employee's taxation, banking or superannuation affairs. (Privacy Act 1988)

Guiding Principles:

The Banyule Community Health Services' confidentiality and privacy policy and procedure is based on the Health Records Act 2001 (Vic) and Privacy Act 1988 (Cth). Under the Health Records Act 2001 (Vic) information must be handled in accordance with the 'Health Privacy Principles'. Under the Privacy Act 1988 (Cth), information must be handled in accordance with the Australian Privacy Principles. These guiding principles are described in the appendices to this policy.

Objectives:

The objectives of the policy are to:

- Ensure professionals comply with relevant professional and legislative requirements in relation to consumer privacy and confidentiality.
- To ensure the service provides confidentiality and privacy in its physical environment.
- To ensure the service has systems to ensure confidentiality and consent in the conduct of student education, audits and research.

Responsibilities:

The **Health Information Officer** is responsible for handling Health Records Access requests. At BCH, the **Executive Assistant** assumes this role. If the Executive Assistant is not available, the CEO will take on these responsibilities. The role of the Health Information Officer is to:

- To facilitate access to health records according to Health Records Act 2001
- To determine if there are any exceptions that apply to the release of information requested.
- To confirm the identity of applicant or status of authorised representative

The **CEO** is responsible for Internal reviews of Health Records Act decisions.

The **Privacy Officer** is responsible for ensuring personal information is managed in accordance with the Privacy Act (1988). At BCH, the **Manager of Community Programs** assumes the role of Privacy Officer. If the Manager of Community Programs is not available, the CEO will take on these responsibilities. The **role of the Privacy Officer** is to:

- Assist with compliance with the Privacy Act.
- Develop policies concerned with the management of personal information.

- Ensure an internal complaints process is available

The Administration Manager is responsible for:
- Overseeing the management of secure client information management systems and file management
- Ensuring that information collected through the Service Access team is collected according to the health privacy principles

The Human Resources Coordinator is responsible for:
- Overseeing the management of secure human resources information systems and the privacy and confidentiality of employee personal and health information
- Ensuring that information collected through Human Resources is collected according to the Australian Privacy Principles

All management and staff are responsible for:
- Maintaining up to date, accurate and complete health records
- Making the procedure for access to health information (BCH *Access to Health Records Procedure*) available to clients on request

Policy Review and Monitoring:

This policy is reviewed triennially or sooner as required.

Legislation

Information Privacy Act 2000 (Vic)
Health Records Act 2001 (Vic)
Health Services Act 1988 (Vic)
Human Services (Complex Needs) Act 2009 (Vic)
Child Wellbeing and Safety Act 2005 (Vic)
Mental Health Act 1986 (Vic)
Privacy Act 1988 (Cth)
Healthcare Identifiers Act 2010 (Cth)
National Health Security Act 2007 (Cth)
Statutory Guidelines on Research issued by the Health Services Commissioner February 2002

Related Documents

BCH *Confidentiality and Privacy Procedure*
BCH *Access to Health Records Procedure*
BCH *Client Health Records Procedure*
BCH *Code of Conduct*

Related Compliance Register(s) in Advent Manager

NATIONAL – Australian Privacy Principles
NATIONAL – Confidentiality of Persons Under Health Observation
NATIONAL – Personal Information in Emergencies and Disasters
Vic – Access to Health Information

Vic – Confidentiality
Vic – Confidentiality for Complex Needs Clients
Vic – Confidentiality for Mental Health Patients
Vic – Health Privacy Principles

Appendices

Appendix 1 – Health Privacy Principles
Appendix 2 – Australian Privacy Principles.

BANYULE Community Health

Human Rights Assessment Form

Section A and B to be completed by the policy or procedure developer

Date:	Policy Developer:
13/01/2012	Quality Coordinator

A. ASSESSMENT OF COMPATIBILITY	
Please indicate which of the following human rights described in the Victorian *Charter of Human Rights and Responsibilities Act* is relevant to this policy / procedure? (tick)	
Recognition and Equality before the law	
Right to Life	✓
Protection from torture and cruel, inhuman or degrading treatment	✓
Freedom from forced work	
Freedom of movement	
Privacy and reputation	✓
Freedom of thought, conscience, religion and belief	
Freedom of expression	
Peaceful assembly and freedom of association	
Protection of families and children	
Taking part in public life	
Cultural rights	
Property rights	
Right to liberty and security of person	
Humane treatment when deprived of liberty	
Children in the criminal process	
Fair hearing	
Rights in criminal proceedings	
Right not to be tried or punished more than once	
Retrospective criminal laws	
Is this policy/procedure compatible with the human rights indicated above?	☑ Yes ☐ No
If Yes, briefly describe how it is compatible	
The Privacy and Confidentiality Policy and related procedures support the right of clients to life by providing mechanisms that enhance the quality and safety of services provided. It protects clients from torture and cruel, inhuman or degrading treatment by ensuring that clients are treated at all times with dignity and privacy. It upholds the right of privacy and reputation by ensuring that all health information managed by BCH is managed in accordance with privacy legislation, and that staff are active participants in the protection of client privacy.	

If No, describe the nature and extent of incompatibility

Human Rights Assessment Form

B. REMEDIAL ACTION
Describe any action that can be taken to redress any incompatibility

Section C to be completed by the Management Team or Board of Management

C. APPROVAL	
☐ This policy/procedure does not require further change to be compatible with the Victorian Charter of Human Rights and Responsibilities and was/was not approved. ☐ This policy/procedure was/was not approved with the following modifications to ensure human rights are preserved:	
Date: 29th March 2012	Approving Body: Board of Directors

Appendix 1: Health Privacy Principles

Principle	Name	Description
HPP1	Collection	Health information is only collected if necessary for the performance of a function or activity and with consent. Individuals must be notified about what will be done with the information and that they can gain access to it.
HPP 2	Use and Disclosure	Health information is only used or disclosed for the primary purpose for which it was collected, or a directly related secondary purpose the person would reasonably expect. Consent is needed for any other use.
HPP 3	Data Quality	Reasonable steps are taken to ensure health information is accurate, complete, up-to-date and relevant to the functions performed.
HPP 4	Data Security and Retention	Health information is to be safeguarded against misuse, loss, unauthorised access and modification.
HPP 5	Openness	Policies on management of health information are to be clearly documented, expressed and made available to anyone who asks for them.
HPP 6	Access and Correction	Individuals have the right to seek access to health information about them, and to correct it if it is inaccurate, incomplete, misleading or not up-to-date.
HPP 7	Identifiers	A number is only assigned to a person if it is necessary to carry out functions efficiently
HPP 8	Anonymity	Individuals are to be given the option of not identifying themselves when entering transactions with organisations where this is lawful and practicable.
HPP 9	Transborder Data Flows	Health information will only be transferred out of Victoria if the organisation receiving it is subject to laws substantially similar to the Health Privacy Principles
HPP 10	Transfer/Closure of practice of health service provider	Notice must be given of transfer or closure of services to past service users
HPP 11	Making information available to another service provider	Health information relating to an individual will be made available to another health service provider if requested by the individual.

Appendix 2: Australian Privacy Principles

Principle	Name	Description
APP 1	Open and transparent management of personal information	Personal information is managed in an open and transparent way. Policies on privacy and the management of personal information must be up-to-date and available free of charge and in an appropriate form for those who request it. The organisation must be able to deal with enquiries or compliants about the APPs.
APP 2	Anonymity and pseudonymity	Individuals have the option of not identifying themselves, or using a pseudonym except for where this is impracticable for the organisation to deal with that individual
APP 3	Collection of solicited personal information	Personal information (other than sensitive information) will not be collected unless the information is necessary for the organisation to perform its functions or directly related functions and activities. Sensitive information will not be collected unless the individual consents and the information is necessary for the organisation to perform its functions, or the collection is authorised or required by Australian law or a court/tribunal order. Information will only be collected by lawful and fair means. It will be collected only about the individual and from the individual, unless otherwise consented to by the individual, required by law or order, or it is unreasonable and impractical to do so.
APP 4	Dealing with unsolicited personal information	If an organisation receives unsolicited personal information that it would not have otherwise collected, the organisation will take steps to destroy the information or ensure that it is de-identified.
APP 5	Notification of the collection of personal information	At the time of collection of personal information, or as soon as possible after, the organisation must notify the individual that the information has been collected, the purpose for which it will be used, any other organisation or body that the organisation usually discloses personal information of the kind collected, how the individual may access that personal information, and that the organisation's policy describes how a complaint about privacy can be made.
APP 6	Use or disclosure of personal information	Personal information held about an individual that was collected for a particular purpose, can only be used for that purpose unless the individual has consented to the use and disclosure, or the individual would reasonably expect the organisation to use or disclose the information for a secondary purpose.
APP 7	Direct marketing	Personal information about an individual must not be used or disclosed for the purpose of direct marketing, unless an individual would reasonably expect the organisation to disclose the information for that purpose and the organisation provides a simple means for the individual to request that they are not sent marketing information.
APP 8	Cross-border	Before an organisation discloses personal information to

Appendix 2: Australian Privacy Principles

	disclosure of personal information	an overseas recipient, it must take steps to ensure that the overseas recipient does not breach APPs, unless the agency reasonably believes that the disclosure is necessary for enforcement purposes of an enforcement agency.
APP 9	Adoption, use or disclosure of government related identifiers	An organisation must not adopt a government related identifier for an individual as its own identifier of an individual unless required or authorised by Australian law or it is reasonably necessary to verify the identity of the individual.
APP 10	Quality of personal information	An organisation must take such steps as are reasonable to ensure that the personal information it collects is accurate, up to date, and complete.
APP 11	Security of personal information	An organisation must take such steps as are reasonable to protect the personal information is holds about individuals from misuse, interference and loss; and from unauthorised access, modification or disclosure. Where the personal information collected by the organisation is no longer needed for use or disclosure, and the organisation is not required by an Australian law or court or tribunal order to retain the information, the organisation must take steps to destroy the information or ensure that it is otherwise de-identified.
APP 12	Access to personal information	An individual must be provided with access to their personal information on request, unless the organisation reasonably believes that providing access would pose a serious threat to the life, health or safety of the individual or the public; giving access would have unreasonable impact on the privacy of other individuals; the request is frivolous or vexatious; the information relates to existing or anticipated legal proceedings and the information would not be available through those proceedings; or giving access would be unlawful.
APP 13	Correction of personal information	If personal information held about an individual is found to be inaccurate, out-of-date, incomplete, irrelevant or misleading, or the individual requests that information be corrected, the organisation will take steps to correct that information. If that information has been previously disclosed to a third party, the organisation must take steps to notify the third party of the correction unless it is unlawful or impracticable to do so. If an organises refuses to correct information it must explain that decision in writing to the individual, and the mechanisms for complaint about the refusal.