BEECHWORTH HEALTH SERVICE

Organisational Wide Policy
- Org 57 – Information Privacy

Policy Statement

Beechworth Health Service (BHS) will maintain the privacy and confidentiality of patients, residents, clients, volunteers and employees of BHS in accordance with applicable legislation, including the *Health Services Act 1988* (Vic), the *Mental Health Act 2014* (Vic), the *Privacy and Data Protection Act 2014* (Vic), the *Health Records Act 2001* (Vic), and the *Privacy Act 1988* (Cth).

Process

BHS has access to identifying personal information, which includes health information and sensitive information about patients, residents, clients and staff. Collecting, using and sharing personal information is a legitimate part of providing health care services and keeping people safe. BHS will collect, use and share information only in accordance with the law.

Privacy Principles and definitions

There are 10 Information Privacy Principles (**IPPs**) set out in the *Privacy and Data Protection Act 2014 (Vic),* and 11 Health Privacy Principles (**HPPs**) defined under the *Health Records Act 2001 (Vic).* The IPPs and HPPs are similar (but in most cases the requirements under the HPPs are more robust).

Section 141 of the *Health Services Act 1988* (Vic) and section 346 of the *Mental Health Act* 2014 (Vic) specifically prohibit disclosure of identifying patient or client information except in specified circumstances, and will override any IPPs or HPPs regarding disclosure of such information.

Otherwise the *Health Records Act 2001* (Vic) and HPPs apply to the collection, use, storage and other handling of health information, and the *Privacy and Data Protection Act 2014* (Vic) and IPPs apply to the collection, use, storage and other handling of personal information that is not health information (for example, personal information relating to staff or service providers that does not include health information) and sensitive information.

Access to and correction of personal information held by BHS is governed primarily by the *Freedom of Information Act 1982* (Vic). See the BHS Freedom of Information Policy for further information.

Personal information means 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.

Health information means information or an opinion (that is also personal information) about:

(a) the physical, mental or psychological health (at any time) of an individual;
(b) a disability (at any time) of an individual; or
(c) an individuals expressed wishes about the future provision of health services to him or her; or
(d) a health service provided, or to be provided, to an individual; or
(e) other personal information collected to provide, or in connection with the provision of, a health service; or

(f) 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
(g) genetic information about an individual that is, or could be, predictive of the health of the individual or a genetic relative of the individual,

Sensitive information (for the purposes of the IPPs) means a subset of personal information which is given specific protections under the IPPs. Sensitive information is information or an opinion (that is also personal information) about an individual's:

(a) racial or ethnic origin; or
(b) political opinions; or
(c) membership of a political association; or
(d) religious beliefs or affiliations; or
(e) membership of a professional or trade association; or
(f) membership of a trade union; or
(g) sexual preferences or practices; or
(h) criminal record

The requirements under the above laws can be addressed as one set of 11 principles that define the information privacy requirements of BHS staff, as below.

1. Collection.

BHS will only collect personal information or health information if it is necessary to perform its functions and activities, and this is in accordance with the permitted circumstances under the IPPs and HPPs, which include where:

- The individual has consented (this also refers to private details of staff and volunteers such as address, phone and roster related information);
- The collection of information is required, authorised or permitted by law;
- The information is necessary to provide a health service and the individual is incapable of giving consent due to age, disability, mental disorder, etc., and there is no authorised representative available to provide consent;
- The information has been disclosed to BHS for a secondary purpose directly related to the primary purpose for which it was collected from the individual, and the individual would reasonably expect BHS to collect the information for the secondary purpose;
- The information is collected about a deceased or missing person or a person involved in an accident who is unable to consent, and the health information is collected for the purposes of identifying the individual and contacting family members, unless this is against the expressed wishes of the individual before they died, went missing or became incapable of providing consent;
- The collection is necessary for research in the public interest and it is not practicable to seek the individual's consent or to use de-identified information, and the research is conducted in accordance with guidelines produced by the Health Complaints Commissioner;
- The collection is by or on behalf of a law enforcement agency and BHS reasonably believes that the collection is necessary for the law enforcement function and advice has been obtained from BHS's Privacy Officer (CEO) to confirm collection is in accordance with the law; or
- The collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

However, sensitive information may only be collected in the following more limited circumstances:

- Where the individual has consented;
- Where the collection is required or authorised under law;
- Where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual:

    - is physically or legally incapable of giving consent to the collection; or
    - physically cannot communicate consent to the collection;
- Where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim; or
- Where:
    - the collection:
        - is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
        - is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
    - there is no reasonably practicable alternative to collecting the information for that purpose; and
    - it is impracticable for BHS to seek the individual's consent to the collection.

Collection must be lawful, by fair means, and not unreasonably intrusive. BHS will collect information directly from individuals where possible, and if information is collected from a third party, BHS will take reasonable steps to provide notice to the individual that their information has been collected.

2. Use and Disclosure

BHS may only use or disclose personal or health information about an individual for the primary purpose for which it was collected or a directly related purpose the individual would reasonably expect.

Health information can also be used or disclosed for a secondary purpose in limited circumstances under the applicable laws, which include where:

- The individual has consented to the use or disclosure.
- The use or disclosure is required or authorised by or under law.
- This is a disclosure required in connection with the further treatment of the individual.
- The use or disclosure is necessary for research in the public interest, and it is not practicable to seek the individual's consent or to use de-identified information, and this is in accordance with guidelines issued by the Health Services Commissioner, and in the case of disclosure, BHS reasonably believes the recipient will not disclose the information and it will not be published in a form which identifies any individuals, and this research is approved by a HREC.
- BHS believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety and welfare or a serious threat to public health, public safety or public welfare, and is in accordance with guidelines issued by the Health Complaints Commissioner.

3. Data Quality

BHS will take reasonable steps to ensure that personal or health information it collects, uses or discloses is accurate, complete, and up to date.

4. Data Security

BHS will take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modifications or disclosure.

BHS will take reasonable steps to destroy or permanently de-identify health information if it is no longer needed.

In relation to patient records and other health information it holds, BHS will only delete health information about an individual if:

- the deletion is permitted by law
- if the health information was collected while the individual was a child, after the child reaches 25 years or
- in any other case, it is more than 7 years after the last occasion on which the health service was provided

Note, however, that BHS is subject to potentially longer periods for retention of patient records in accordance with public records disposal authorities issued by the Public Records Office of Victoria (under the *Public Records Act 1973* (Vic)).

If BHS deletes any health information, it will record the details of the name of the individual, the period it related to and the date the information was deleted. A record containing these details must also be made if BHS transfers health information to another organisation and does not continue to hold a record for that individual.

Access to record keeping and digital record systems is controlled and staff and authorised external users will have access only to systems that their duties require.

Paper records will be securely stored and access will only be granted to authorised personnel.

5. Openness

BHS will document policies on its management of health information. BHS will make these policies available to anyone who asks for it.

On request by a person, BHS must take reasonable steps to let the person know generally, what sort of health information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Access and Correction

Access to and correction of information that BHS holds will occur in accordance with the *Freedom of Information Act 1982* (Vic) (**FOI Act**).

Individuals have the right to seek access to their personal information and make corrections to that information, but that right is not absolute under the FOI Act. BHS will, on request, provide patients, residents, clients and staff with access to information it holds about them and allow them to make corrections, subject to any applicable exemptions under the FOI Act. Please see the BHS Freedom of Information Policy.

BHS will correct health information about an individual so that it is accurate; however, it cannot delete health information, even if it is inaccurate, unless it is permitted by law (for example, the relevant retention periods have been met as discussed above).

7. Unique Identifiers

BHS will only assign unique identifiers if it is necessary for BHS to carry out any of its functions efficiently.

8. Anonymity

Wherever it is lawful and practicable, individuals will have the option of not identifying themselves when entering into a transaction with BHS.

9. Transborder Data Flows

BHS may only transfer information about an individual to someone (other than the individual) who is outside of Victoria if this is in accordance with the principles for disclosure discussed above, and one of the following applies:

- BHS reasonably believes the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information that are substantially similar to the HPPs and IPPs.
- The individual consents to the transfer
- The transfer is necessary for the performance of a contract between the individual and BHS, or for the implementation of pre-contractual measures taken in response to the individual's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between BHS and a third party
- All of the following apply:
    - the transfer is for the benefit of the individual
    - it is impracticable to obtain the consent of the individual to that transfer
    - If it were practicable to obtain that consent, the individual would be likely to give it.
- BHS has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles.

10. Transfer or Closure of BHS

HPP 10 sets out the procedure which must be followed if BHS's services are transferred or closed, or sold. For further information how personal information should be handled in the event of transfer of closure of BHS services, and the applicable Health Complaints Commissioner guidelines see:

https://hcc.vic.gov.au/sites/default/files/2021-04/hra_statutory_guidelines_transfer_or_closure.pdf

11. Making Information Available to another Health Service Provider and / or responding to the Department of Health and Child Protection and other Prescribed Information Sharing Entities.

If an individual requests BHS to make health information relating to the individual to another health service provider, or authorises another health service provider to request BHS to make information available to that health service provider about the individual, BHS will provide copies or a summary of the health information to that health service provider.

BHS will comply with the requirements of this principle as soon as practicable.

Alignment with the Victorian Family Violence Multi-Agency Risk Assessment and Management (MARAM) Framework

The Victoria Royal Commission 2016 into Family Violence, found that effective information sharing is crucial in keeping victims safe and holds perpetrators to account.

BHS acknowledges the introduction of the Multi-Agency Risk Assessment and Management Framework (MARAM), which will continue previously implemented work under the Strengthening Hospital Response to Family Violence (SHRFV).

The MARAM Framework provides best practice guidelines for family violence risk assessment and management, based on current evidence and research. It aims to establish a system-wide shared understanding of family violence and collective responsibility for risk assessment. This allows the facilitation of consistent, effective, safe responses and management for people experiencing family violence.

The MARAM Framework is underpinned by ten principles:

Family violence involves a spectrum of seriousness of risk and presentations, and is unacceptable in any form, across any community or culture.

Professionals should work collaboratively to provide coordinated, effective risk assessment and management responses. This includes early intervention when family violence first occurs to avoid escalation into crisis and additional harm.

During risk assessment and management of family violence disclosures, professionals should be aware of the determinants of family violence, predominantly gender inequality, structural inequality and discrimination.

Victim survivors must be respected and empowered. Professionals need to partner with them as active decision-makers in risk assessment and management. This includes support to access and participate in law processes that enable fair and just outcomes.

Family violence may have serious impacts on the current and future physical, spiritual, psychological, developmental, emotional safety and wellbeing of children, who are directly or indirectly exposed to its effects. Children should be recognised as victim survivors in their own right.

Services provided to child victim survivors should acknowledge their unique experiences, vulnerabilities and needs, including the effects of trauma and cumulative harm arising from family violence

Services and responses provided to people from Aboriginal communities should be culturally responsive and safe. Aboriginal understanding of family violence and rights to self-determination and self-management, needs to be recognised as impacts of historical and ongoing events of colonisation, systemic violence and discrimination.

Services and responses provided to diverse communities and older people should be accessible, culturally responsive, safe, client-centred, inclusive and non-discriminatory.

Perpetrators should be encouraged to acknowledge and take responsibility to end their violent, controlling and coercive behaviour. Service responses to perpetrators should be collaborative and coordinated through a system-wide approach that creates opportunities for perpetrator accountability.

Family violence used by adolescents is a distinct form of family violence. It requires a different response due to their age and the possibility that they are also victim survivors of family violence.

Breach of Privacy

Any suspected infringement of privacy will be reported using the VHIMs (Riskman) incident reporting system and will be escalated to the CEO who will coordinate an investigation and consider the recommendations of that investigation.

Infringements of privacy in breach of this policy may result in disciplinary action.

Notifiable Data Breaches

BHS will investigate all suspected infringements of privacy and determine if the breach constitutes a breach notifiable to either The Department of Health (DoH), the Office of the Victorian Information Commissioner (OVIC), or the Office of the Australian Information Commissioner (OAIC).

Infringement of privacy involving clients of community health will require notification to the Department of Health 1 business day. The infringement is to be reported using the web-based tool located at:

https://providers.dhhs.vic.gov.au/reporting-incidents

Infringement of privacy involving the disclosure of tax-file numbers or information likely to cause serious harm to one or more individuals are notifiable to both OVIC and OAIC.

For further information on notification to OVIC see:

https://www.cpdp.vic.gov.au/images/content/pdf/privacy_info/20180216-OVIC-NDB-scheme-guidance.pdf

For further information on notification to OAIC see:

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify

Collection and use of staff sign in information

BHS uses the LoopSafe system which enables automated sign-in processes for staff using face identification technology. As part of the LoopSafe system 'LoopKiosks' will be in place across BHS for staff to sign in.

The LoopKiosk is a device which allows people to sign themselves in and out of BHS. It will provide an accurate record of everyone onsite at any point in time, which is particularly important in the event of an emergency, and to ensure that all people onsite are authorised and safe to be there.

The key features of LoopSafe and the LoopKiosks are real time face identification for sign in, attestation (e.g., health screening questions) and temperature testing. This system also integrates with staff timesheet systems for payroll purposes.

The LoopSafe technology identifies individuals in real-time within the system's hardware. The LoopSafe identification algorithm produces a cached string of numbers stored in an encrypted database to perform face identification. These numbers are only useful to the LoopSafe algorithm and cannot be used by anything else. This means no images are required to be saved and stored by LoopSafe after the identification process is complete. Any biometric information is de-identified, encrypted and unique to LoopSafe devices.

This process for sign in will result in BHS collecting from staff both personal information (in respect of sign in) and health information (for example, in respect of answers to health screening questions). This information is only accessible by BHS and no information is transferred to, shared with, or accessible by any third-party at any time. Further, all information is stored in Australia.

Use of the LoopSafe system will be in accordance with the applicable privacy laws and this policy, namely:

- The collection of staff personal and health information via this sign in process is necessary for BHS to perform its functions and activities, including its HR/payroll activities, and also ensuring a safe workplace for staff, patients and visitors in accordance with its duties under law.
- The collection of this information will only occur with staff consent and directly from staff members.
- The process for collection is not unreasonably intrusive and will only collect the minimum information necessary to help ensure that BHS has an accurate record of attendance and can provide a safe workplace visitors in accordance with its duties under law.
- The use of this information by BHS will only be for the above attendance and workplace safety purposes. BHS will seek further staff consent should it wish to use the information collected for any other purposes.
- Staff information will be stored securely on BHS's own ICT systems and will not be disclosed to or accessible by any third parties.

Outcome

BHS will comply with all legislation relating to information privacy.

Definitions

Client Where persons are referred to as 'client', this means a patient, client or consumer of the service however otherwise named, and specifically means consumers of the Primary Health Outpatient services, the District Nursing service, the Planned Activity Groups, and the National Disability insurance Scheme.

See also this policy above for the definitions of: **personal information**, **health information**, and **sensitive information**.

Policy Risk Management

Goal	Risk	Rating (With controls as per this policy)	Required actions
BHS will comply with all legislation relating to information privacy.	That BHS does not comply with all legislation relating to information privacy.	Freq = Unlikely Conseq = Moderate Rating = Medium (6)	• Specify management accountability and responsibility • Monitor trends • Develop quality improvement plans

Policy Quality Improvement Action Plan

Specify accountability and responsibility	• Responsibility for governance of this policy is assigned to the Finance, Resource and Information Technology Committee.
Monitor Trends	• All suspected breaches of information privacy will be reported on VHIMs (Riskman).
Education	• This Policy will be displayed on the staff intranet • The OHS Committee will monitor the use of this policy. • Education will be conducted at staff orientation • Education sessions will be conducted from time to time as deemed necessary
Quality Improvement	Quality Improvement to this policy will be informed at review by: • Feedback (if any) • Audit results • Department Policy • Industry Guidelines • Incident reports

Document Control

Standards	• NSQHSS - Standard 1Clinical Governance Standard • RAC – Standard 1 consumer Dignity and Choice. • NDIS – Standard 2.4 Information Management
References	• Health Records Act 2001 (Vic) • Privacy and Data Protection Act 2014 (Vic) • Privacy Act 1988 (Cwlth) • Aged Care Act 1997 • Health Records Act 2001 (VIC) • BHS Policy – Freedom of Information • BHS Policy -Code of Conduct • NDIS Quality and Safeguards Commission (2018) NDIS Practice Standards and Quality Indicators • Victorian Government, (2018), Family Violence Multi-Agency Risk Assessment and Management Framework. A shared responsibility for assessing and managing family violence risk. Vic. Gov. Melbourne. Available from https://www.vic.gov.au/family-violence-multi-agency-risk-assessment-and-management-framework
Approving Committees	Finance, Resources & IT Services Committee FRITS Approval Date: 28/06/2022 Finance & Audit Committee Approval Date: 21/09/2021 Board of Management (BOM) Approval Date: 23/09/2021
Contact Point	M. Ashcroft, Chief Executive Officer
Review Dates	Issue Date: 01/08/2002 Last Review: 28/06/2022 Next Review: 28/06/2025