# Organisational Wide Policy
# - Org 57 – Information Privacy

## Policy Statement

Beechworth Health Service (BHS) will uphold the Victorian information privacy rights established by the *Privacy and Data Protection Act 2014 (Vic),* the *Health Records Act 2001 (Vic),* and the *Privacy Act 1988 (Cwlth),* for patients, residents, clients, and employees of the health service.

## Process

BHS has access to personal information, (which includes sensitive information) and health information about patients, resident's clients and staff. Sharing information is a legitimate part of providing health care services and keeping people safe. BHS will share information only in accordance with the law.

### Privacy Principles

There are 9 Information privacy principles defined under the *Privacy and Data Protection Act 2014 (Vic),* and 11 Health privacy principles defined under the *Health Records Act 2001 (Vic).* The 2 sets of privacy principles are strongly aligned, and the requirements and 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 information if it is necessary to perform its functions and activities, and at least one of the following applies:

- The individual has consented
- The collection 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 collection is for a secondary purpose directly related to the primary purpose and the individual would reasonably expect BHS to collect the information for the secondary purpose
- BHS has reason to suspect that unlawful activity has been, or is being undertaken and collect the information as a necessary part of its investigation of the matter or in reporting its concerns to the relevant persons or authorities.
- 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 and is conducted in accordance with guidelines produced by the Health Services 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 laws.
- The collection is necessary for the establishment, exercise or defence of a legal or equitable claim

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 if:

- The individual has consented to the use or disclosure.
- The use or disclosure is required or authorised by or under law.
- The use or disclosure by a health service provider 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 use or disclosure is necessary for research in the public interest when it will be published in a non-identifiable format and it is not practicable to seek the individual's consent and in the case of disclosure, BHS reasonably believes the recipient will not disclose the information.
- 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 Services Commissioner.
- BHS has reason to suspect that unlawful activity has been or is being engaged in and uses or discloses the health information to investigate the matter or to report concerns to relevant persons or authorities (and if it relates to a health service provider eg Community Services, it is not a breach of confidence)
- A law enforcement agency has requested health information and authorisation has been obtained from the BHS Privacy Officer to assist the law enforcement agency.

**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

BHS will only delete 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, more than 7 years after the last occasion on which the health service was provided

BHS 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**

Individuals have the right to seek access to their personal information and make corrections. BHS will, on request, provide patients, residents, clients and staff with access to information it holds about them and allow them to make corrections unless an exemption applies at law.

BHS will provide patients, clients, residents and staff with access to information it holds about them, unless there is an exception that applies under the Information Privacy Principles or Health Privacy Principles. To make a request for access to personal information, please see the BHS Freedom of Information Policy.

BHS will correct health information about an individual so that it is accurate; however it will not delete the information, even if it is inaccurate.

**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:

- 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 these Health Privacy Principles.
- 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 the Practice of BHS

This principle sets out the procedure which must be followed if BHS practices are transferred or closed, or sold. For further information how personal information should be handled in the event of Transfer of closure of practice see:

https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-change-of-business-circumstances-or-closure-of-a-health-service

### 11. Making Information Available to another Health Service Provider

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.

### Breach of Privacy

Any suspected infringement of privacy will be reported using the VHIMs (Riskman) incident reporting system.

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 and Human Services (DHHS), 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 and Human services within 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 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

## 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.

### 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<br>Conseq = Moderate<br>Rating = Medium (6) | • Specify management accountability and responsibility<br>• Monitor trends<br>• 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<br>• The OHS Committee will monitor the use of this policy.<br>• Education will be conducted at staff orientation<br>• 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:<br>• Feedback (if any)<br>• Audit results<br>• Department Policy<br>• Industry Guidelines<br>• Incident reports |

# Document Control

| | | | |
|---|---|---|---|
| **Standards** | • NSQHSS - Standard 1Clinical Governance Standard<br>• RAC – Standard 1 consumer Dignity and Choice.<br>• NDIS – Standard 2.4 Information Management | | |
| **References** | • Health Records Act 2001 (Vic)<br>• Privacy and Data Protection Act 2014 (Vic)<br>• Privacy Act 1988 (Cwlth)<br>• Aged Care Act 1997<br>• Health Records Act 2001 (VIC)<br>• BHS Policy – Freedom of Information<br>• BHS Policy -Code of Conduct<br>• NDIS Quality and Safeguards Commission (2018) NDIS Practice Standards and Quality Indicators | | |
| **Approving Committees** | Finance, Resources & IT Services Committee<br>(FRITS)/Finance & Audit Committee<br>Board of Management (BOM) | | Approval Date: 27/03/2018<br>Approval Date: |
| **Contact Point** | M. Ashcroft, Chief Executive Officer | | |
| **Review Dates** | Issue Date: 01/08/2002 | Last Review: 13/8/2020 | Next Review: 13/8/2023 |