

INFORMATION MANAGEMENT AND PRIVACY POLICY

POLICY PURPOSE:

The intent of this policy is to demonstrate the Better Health Company's (BHCo) commitment to identifying and managing knowledge and information in a way that facilitates organisational learning, organisational, operational and project objectives and supports continuous improvement and ongoing development whilst at the same time meeting legislative requirements.

1. POLICY DETAILS

Information management is an overarching term that encompasses the systems and processes within an organisation for the creation, access, use and storage of information and turn information to Knowledge. BHCo handles, holds, analyses and permits access and correction of personal information in accordance with the Australian Privacy Principles. We provide information for users on our website about the privacy of your information and how we protect that privacy.

1.1 Information Privacy

Personal information

Personal information means information or an opinion (including information or an opinion forming part of a database) about an individual (Office of the Federal Privacy Commissioner, 2001). What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances. For example, personal information could include:

- a name or address
- bank account or payment details
- photos or videos
- information about an individual's health, wellbeing, opinions or feedback

Note: information does not have to include an individual's name to be personal information. For example, in some cases, a date of birth and post code may be enough to identify a person.

Sensitive information

Sensitive information is a subset of personal information with additional requirements under the Privacy Act. Sensitive information is defined in the Privacy Act as 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, or criminal record that is also personal information; health information about an individual, genetic information about an individual, biometric information that is to be used for the purpose of automated biometric verification/identification and biometric templates. The Managing Director provides clarification if staff are unsure whether information is confidential or sensitive.

Types of personal information collected and held by Better Health Company:

Personal information

BHCo holds internal information such as employee qualifications and health status, salary information, meeting minutes, financial reports and bank account details, business objectives and plans, as well as external information such as funding agreements, population health information, meeting minutes, service provider information and stakeholder information;

Sensitive information

BHCo does not hold a full patient health record but through certain programs, where informed consent is given, does have access to limited patient information e.g. a referral for services. In these instances information is treated confidentially with the staff member ensuring the client is aware of the information being recorded, the purpose of recording the information, and which information (if any) will be transmitted to other bodies (including funding bodies) and for what purpose. Client information will only be used for the purposes for which it is collected, unless the information has been de-identified or consent has been obtained to use it for other purposes. Other sensitive information may be held by BHCo e.g. professional qualifications or racial or ethnic origin

Limits to confidentiality

Confidentiality exists between the client and the agency providing the service. In the following situations, duty of care considerations can override confidentiality:

- when there is an obligation not to conceal an intended or actual crime including child abuse, theft, assault, fraud
- when the client or a third party may be in danger or come to harm if key information is withheld
- when there may be a duty of care consideration to inform a third party

Informed consent

Informed consent means that the client:

- understands the need to exchange personal information about them
- knows what personal information will be exchanged
- knows with whom or what agency the information will be exchanged
- agrees to the exchange

BHCo only shares and exchanges personal information with the client's informed consent. Consent must be recorded on the Program Consent Form which is held by in hard copy by the partner agency. In situations where the agency believes that the client may not have the capacity to give informed consent because of their age, mental state or disability, will attempt to secure substitute consent from the client's guardian or appointed representative. In situations where the client is unwilling to give consent, the need for privacy will be balanced against the organisation's duty of care responsibilities.

How Better Health Company collects personal information:

BHCo endeavours to collect information directly from the individual. However, there may be times when personal information is collected from a third party. If this occurs, such collection will be in accordance with the APPs. As well as collecting personal information directly BHCo or our partner agencies may also collect personal information through other individuals or organisations acting on our behalf, including those such as contracted service providers.

When collecting personal information we may do this through using forms (either electronic or hard copy), online portals, other electronic or paper correspondence (including emails and written correspondence) and at times verbal conversations or interviews.

Unsolicited information

Unsolicited personal information is provided without it being requested. Unsolicited personal information that BHCo could not collect through its normal processes is de-identified or destroyed where lawful and reasonable to do so.

How Better Health Company holds personal information:

The Better Health Company is considered to 'hold' personal information where it:

- physically possesses a record containing personal information, or
- has the right to deal with the information, even if it does not physically possess it (such as where the personal information is stored on servers owned by a third party, to which BHCo has access to, or in archived files).

All personal information held by BHCo received in paper form will be stored in a secure, lockable location; if in electronic form, password and firewall protected; accessible by approved staff only and not taken from BHCo offices unless authorised and for a specified purpose.

Personal information held by third parties:

Under the Privacy Act BHCo is required to take measures to ensure that when personal information is to be held by a third party, that the third party complies with the same privacy requirements applicable to BHCo. BHCo has privacy clauses in all of its legal documents, including funding deeds, services contracts and various other ad-hoc arrangements. This is to ensure third parties that BHCo deals with are required to handle personal information in accordance with the APPs.

How BHCO uses and discloses personal information:

Unless an exception applies, BHCo will only use or disclose personal information for the purpose it was collected. The BHCo will only use or disclose personal information for another purpose where it is able to do so in accordance with the Privacy Act. Personal information is used to enable the functions, activities and programs at BHCo including the functioning of advisory groups, recruitment and HR, maintaining stakeholder relationships, managing funding agreements and contracts, programs and projects, undertaking evaluations and audits, financial transactions, complaints management and research.

Access and corrections to personal information

BHCO aims to ensure information it collects uses or discloses is accurate and complete at the time it is collected, and will endeavour to keep it up-to-date e.g. renewing contact details. In the event that individuals wish to access and/or correct errors in their information, where it is reasonable and legal to do so, this will be done within calendar 30 days. If BHCO corrects personal information, at the individual's request, reasonable steps will be taken to notify other agencies or organisations (bound by the Privacy Act) that we have previously disclosed the information to of the correction. However, it may not be possible to correct information which has been de-identified, has been published, or there is a legal requirement not to do so. In such instances, the individual will be informed in writing of the reason why the information cannot be corrected or changed, and the process to make a complaint.

Privacy Breaches

Privacy breaches can be caused by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harm to individuals, agencies and organisations. Consequently, there is no single way of responding to a privacy breach. Each breach will need to be dealt with on a case-by-case basis. All complaints and alleged breaches will be investigated and the complainant will be advised of the outcome.

BHCo will investigate:

- concerns that the personal information contained in a record of a client or stakeholder has been mishandled
- any complaints and/or allegations about a breach of the APPs, and
- all privacy-related matters referred from the Privacy Commissioner

Overseas disclosures

BHCo does not routinely disclose information overseas. Before BHCo can disclose personal information to an overseas recipient, it will take reasonable steps to ensure that the overseas recipient does not breach the APPs (or recipient's equivalent) and will inform the individual of the countries where the disclosure will occur.

Whilst BHCo does not actively share information with overseas organisations, our company data management system is hosted outside Australian borders however is in compliance with current APP's as per our organisational requirements.

Knowledge Management

Knowledge management comprises a range of strategies and practices used to identify, create, symbolise, distribute, and enable adoption of knowledge, with the external sources of information being part of the knowledge capital for BHCO. Effective management of information will enable concise knowledge management by capturing information that is relevant and facilitating the sharing and transmission of knowledge across the organisation.

BHCo will manage intellectual property in a way that maximises the performance of the organisation whilst minimising legal, reputational and financial risk. Where under contracts with funders BHCO is

required to share information and intellectual property, BCo supports and encourages the dissemination and exchange of its information and has no objection to material being reproduced, made available online or electronically but only if it is recognised as the owner of the copyright and if the material remains unaltered.

2. POLICY SCOPE

This applies to all BCo’s operations. This policy will be reviewed every 3 years and in-line with the Policy Review Process.

3. DEFINITIONS

Term	Meaning
Intellectual Property	Intellectual property includes: copyright in all electronic and hard copy literary works, artistic works, logos, computer software, music, videos, databases, surveys, assessment tools, forms and any other works or subject matter in which copyright subsists and may in the future subsist inventions, discoveries and novel designs, whether or not registered or registrable as patents or designs, including developments or improvements of equipment, products, technology, processes, methods or techniques trade and service marks (whether registered or unregistered)
Records	Records are information objects that document business activities and transactions. To be regarded as evidence a record must be complete. Complete records comprise contextual and structural data as well as content data

4. REFERENCES & RELEVANT LEGISLATION

- Privacy Act, 1988 and Australian Privacy Principles 2014
- Privacy Amendment (Private Sector) Act 2000
- Copyright Act 1968 (Cth)
- Copyright Amendment (Digital Agenda) Act 2000 (Cth)
- Designs Act 2003 (Cth)
- Patents Act 1990 (Cth)
- Trade Marks Act 1995 (Cth)
- Australian Charities and Not for Profits Commission Act 2012