Privacy policy

Purpose of the privacy policy

Privacy is about the right of a person to know of and to control information recorded about them as an individual. All persons have a right to have access to such information and to have a say in what happens to information they reveal about themselves. They have a right to withhold that information but often need to reveal facts about themselves for many reasons. If they do reveal information about themselves they have a right to know how such information is to be used and that it will be respected. They are entitled to know why the information is required, who has access to it and how it is to be kept. They are entitled to know what information is held about them and whether that information is correct. If the information held is incorrect, they are entitled to have that error rectified.

This policy has been developed to assist all levels of Boandik's management structure to ensure that Boandik and staff recognise the rights of clients and others to privacy and to ensure that such rights are respected.

The guide is developed in accordance with the Australian Privacy Principles as contained in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012.*

Introduction

Boandik recognises the rights of its employees and clients to privacy. This policy document represents Boandik's commitment to respecting the rights of the individual with respect to privacy considerations and puts in place procedures to ensure that such rights are respected. The policy identifies those rights and Boandik's obligations to individuals, the community, employees and government.

This policy is written in accord with the Australian Privacy Principles. Boandik is an APP entity under the Privacy Act. It has been devised following an examination of the ways and means by which information is collected by Boandik, the reasons for that collection, the way in which such information is stored and the use to which the information is put. It is designed to clearly define and identify the considerations which need to be made to address all areas of risk to the rights of individuals with respect to the collection, storage and use of information held by Boandik.

The system must be reflective of current best practice and accepted standards and therefore shall be reviewed on a continuing basis.

Privacy is integral to all aspects of Boandik's dealings with its employees, clients and others who, from time to time, provide information to Boandik. To be effective this policy must be systematic and applied continuously.

Privacy issues may be addressed at various levels;

- Board and senior management (policy development and compliance)
- Privacy officer (operational systems supportive of strategic goals)
- Individual

At all levels Boandik's obligation, mission statement and objectives with respect to privacy issues must be known and met. This policy addresses strategies that should be considered under the following general areas to ensure that the Australian Privacy Principles are complied with;

- Commitment
- Planning

- Implementation
- Monitoring and evaluation
- Review

The privacy policy will be made available to all stakeholders on the Boandik website.

This document sets out Boandik's privacy policy. It identifies matters to be considered when managing privacy issues regularly dealt with by Boandik and exists to assist in the identification and management of additional issues that may become apparent from time to time. It is intended that this policy be read along with the Australian Privacy Principals and that it be referred to by all personnel of Boandik to ensure that best practice standards in the recognition of privacy matters are adhered to at all times.

Commitment

The Board will document its policy with respect to privacy issues. The policy will include the objectives and Boandik's commitment to maintaining the right to privacy of all persons, with respect to whom Boandik collects, stores, uses or disseminates personal information.

Privacy policy

Boandik recognises its obligation to comply with the Australian Privacy Principles. Boandik acknowledges and is committed to meeting its obligations under those principles to its clients, staff, contractors and the community.

Boandik has established and will maintain systems relevant to the collection, use and disclosure, quality, security, accuracy and correction of personal information provided to Boandik in all areas of its operations and practice.

Definitions

The following definitions, unless otherwise specified are taken from the *Privacy Act 1988* (the "Act").

"Australian privacy principles": means the principles contained in the Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012. These principles are available from the Administration office at Lake Terrace.

"Data breach", occurs when personal information is lost or subjected to unauthorised access, modification, use, disclosure or other misuse.

"Directly related secondary purpose", refers to the use of information which use is directly related to the primary purpose for which the information was collected and the use of the information in the intended manner would be within the reasonable expectation of the person providing the information.

"Employee record"*,* in relation to an employee, means a record of personal information relating to employment. Examples of personal information relating to the employment include:

(a) engagement, training, disciplining or resignation;
(b) termination of employment;
(c) terms and conditions of employment;
(d) employee's personal and emergency contact details;
(e) employee's performance or conduct;
(f) employee's hours of employment;
(g) employee's salary and wages;
(h) employee's membership of a professional or trade association;

(i) employee's trade union membership;
(j) employee's recreation, long service leave, sick, personal, maternity, paternity or other leave;
(k) employee's taxation, banking or superannuation affairs.

"Health information" means:

(a) information or opinion about:
  (i) the health or a disability of an individual; or
  (ii) an individual's expressed wishes about the future provision of health services to him or her; or
  (iii) 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.

"Health service" means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
  (i) to assess, record, maintain or improve the individual's health; or
  (ii) to diagnose the individual's illness or disability or suspected illness or disability; or
  (iii) to treat the individual's illness or disability or suspected illness or disability; or
(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

"Information sharing guidelines – SA Government" summarise , for service providers, the practical framework that supports the provider in appropriate information sharing practice. They provide guidance where there are threats to safety and wellbeing, when consent is and is not given; they outline the process and professional judgements that should underpin the decision making in both circumstances.

"Responsible person" A person is responsible for an individual if the person is:

(a) a parent of the individual; or
(b) a child or sibling of the individual and at least 18 years old; or
(c) a spouse or de facto spouse of the individual; or
(d) a relative of the individual, at least 18 years old and a member of the individual's household; or
(e) a guardian of the individual; or
(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
(g) a person who has an intimate personal relationship with the individual; or
(h) a person nominated by the individual to be contacted in case of emergency.

"Permitted health situation"

1. A *permitted health* situation exists in relation to the collection by an organisation of health information about an individual if:
  (a) The information is necessary to provide a health service to the individual: and
  (b) Either:
    (i) The collection is required or authorised by or under an Australian law (other than this Act); or
    (ii) The information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

2. A *permitted health situation* exists in relation to the disclosure by an organisation of health information about an individual if:
   (a) The organisation provides a health service to the individual; and
   (b) The recipient of the information is a responsible person for the individual; and
   (c) The individual:
      (i) Is physically or legally incapable of giving consent to the disclosure; or
      (ii) Physically cannot communicate consent to the disclosure; and
   (d) Another individual (the *carer*) providing the health service for the organisation is satisfied that either:
      (i) The disclosure is necessary to provide appropriate care or treatment of the individual; or
      (ii) The disclosure is made for compassionate reasons; and
   (e) The disclosure is not contrary to any wish:

"Permitted general situation"

1. A *permitted general situation* exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:
   (a) The entity is an entity of a kind specified in an item in column 1 of the table; and
   (b) The item in column 2 of the table applies to the information or identifier; and
   (c) Such conditions as are specified in the item in column 3 of the table are satisfied.

Permitted general situations

Item	Column 1 Kind of entity	Column 2 Item applies to	Column 3 Condition(s)
1	APP entity	(a) Personal information; or (b) A government related identifier	(a) It is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and (b) The entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
2	APP entity	(a) Personal information; or (b) A government related identifier	(a) The entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and (b) The entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
3	APP entity	Personal information	(a) The entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and (b) The collection, use or disclosure complies with the rules made under subsection (2).
4	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence

			of a legal or equitable claim.
5	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.
6	Agency	Personal Information	Collection, use or disclosure is necessary for the entity's diplomatic or consular functions or activities
7	Defence Force	Personal Information	The entity reasonably believes that the collection ,use or disclosure is necessary for any of the following occurring outside Australia and the external Territories: (a) War or warlike operations; (b) Peacekeeping or peace enforcement (c) Civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

2. The commissioner may, by legislative instrument, make rules relating to the collection, use or disclosure of personal information that apply for the purposes of item 3 of the table in subsection (1).

"Personal information" means information or an opinion (including information or an opinion forming part of a data base), 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.

"Primary purpose" is the main or dominant reason for which Boandik collects personal information

"Secondary purpose" any reason for which information is collected or used that is not the Primary Purpose for its collection and/or use referred to above.

"Sensitive information" means:

(a) information or an opinion about an individual's:
- (i) racial or ethnic origin; or
- (ii) political opinions; or
- (iii) membership of a political association; or
- (iv) religious beliefs or affiliations; or
- (v) philosophical beliefs;
- (vi) membership of a professional or trade association; or
- (vii) membership of a trade union; or
- (viii) sexual preferences or practices; or
- (ix) criminal record;

that is also personal information; or

(b) health information about an individual.

Key concepts

Access: Involves an organisation allowing an individual access to records containing personal information held about them by Boandik. This may include inspecting personal information held or providing a copy of the information.

Collection: An organisation collects personal information if it gathers, acquires or obtains personal information from any source and by any means. This includes information not requested or obtained in error.

Disclosure: In general terms information is disclosed when an organisation releases information to third parties. Disclosure does not include giving information to an individual about themselves – that is "Access".

Use: This refers to the handling of information within an organisation.

Scope

This policy applies to all areas and functions of Boandik which collect, use, disclose, store and/or provide access to Personal Information, including sensitive information and health information about an individual and includes the areas and functions listed below:

- Client entry
- Client care
- Diagnosis and opinions
- Support/life plans
- Client assets, property and resources
- Financial arrangements
- Health and infection control
- Information systems, computers and technology
- Human resources
- Work health and safety
- Security
- Organisation records
- Purchasing and contract management
- Professional advice

Health information is both personal and sensitive information. This policy covers all information collected by Boandik where such information may fall within any of these definitions. The policy covers all forms of records maintained by Boandik and applies to staff, contractors, clients and others who do or may have reason to use any information collected and held by Boandik.

This Policy does not apply to a staff employee record access to which may be gained through the grievance policy of Boandik. Where staff attends Boandik for the provision of a health service any information retained from that attendance is health information and is covered by the terms of this Policy.

Objectives

The objectives of the privacy policy are to ensure:

1. The only personal information collected is that required by Boandik to effectively and properly care/provide services to the client.
2. Personal information which is collected is collected lawfully, fairly and openly, where possible, directly from the individual concerned.
3. The person or persons from whom the personal information is collected know the reason for the information being requested, including any secondary purpose, and of any law requiring the collection of the information.
4. To ensure that all persons from whom personal information is collected are informed of the identity of Boandik and how to contact Boandik with their concerns on privacy matters including how to access personal information held about them.
5. That all persons from whom the personal information is collected are informed of their rights to obtain the records of information provided to Boandik.
6. That there is no unauthorised use or disclosure of personal information. There are certain circumstances where disclosure of personal information is required by law. This includes obligations not to conceal a crime or intended crime and allegations of abuse. There is a clear procedure to be followed if there is a data breach.

7. That all personal information held by Boandik is kept secure.

Responsibilities and accountabilities

1. The chief executive officer and board of directors will be responsible for the establishment and maintenance of the privacy policy.
2. The chief executive officer will be accountable to the board for the day to day oversight of information management including the collection, access, correction, storage, use and disclosure of personal information.
3. The chief executive officer with the approval of the board will appoint a "privacy officer" who will be responsible to manage the collection, access, correction, storage, use and disclosure of personal information and may seek advice from such appropriate professionals as deemed appropriate including specialist consultants, legal counsel and/or other persons qualified to assist in privacy issues.
4. The chief executive officer will ensure that privacy is a consideration in all projects dealing with personal information and will ensure that a privacy impact assessment is undertaken during the design phase of the project.
5. Managers, including the chief executive officer, will be responsible to consult and communicate with relevant personnel on issues relating to privacy.
6. All employees of Boandik will be responsible and accountable for their role in ensuring that privacy principles are complied with.
7. The executive team have been appointed as the data breach response team.

Collection of information

1. Staff of Boandik are authorised to collect only that information which is necessary for the performance of the service requested of Boandik by the client. If information is given to staff that is irrelevant to such purpose or purposes it should not be recorded or if recorded shall be destroyed by the staff member as soon as possible after its collection. (See "destruction of information" below).
2. Information may be collected for a permitted general situation or a permitted health situation.
3. Information should be collected directly from the client. If it is not possible for any reason to collect the information from the client directly a responsible person may be requested to provide the information needed. (See "collection of information from third parties" below).
4. At any time staff collect personal information, or as soon as possible thereafter, staff shall identify themselves to the client by their first name and shall identify their position in Boandik and the purpose for which they are collecting the information.
5. When personal information is initially being collected from an individual staff requesting such information will:

    (a) Identify themselves and their position within Boandik and, if necessary, give the name of Boandik;
    (b) If not already done so, provide details to the client on how Boandik may be contacted;
    (c) Advise the client of the primary purpose for which the information is being collected and any directly related secondary purpose for which such information may be used or disclosed;
    (d) Advise the client of their right to access information held by Boandik in respect to them;
    (e) If the information being collected is to be passed on to another organisation the staff shall advise the client accordingly and seek the client's consent for the information to be passed on. Such consent shall be placed on the file with the information recorded and, if reasonably possible, checked by the client and signed by them to authorise such disclosure;

(f) If any legal requirement has been imposed requiring the collection of information from the client this fact is to be identified to the client;

(g) The client should be advised of the consequences likely to flow to the client if any information requested of the client is not provided.

(h) The client should be requested to advise of any circumstance which may lead to inadvertent release of information to persons who the client does not want information to be released to (see contact procedures below).

6. Where the consent of the individual is requested for the use and or disclosure of personal information such consent must be given separately from any consent for treatment or other service provided by Boandik. Consent given with respect to treatment is not consent to deal with information about the individual.
7. Where possible, prior to the client attending Boandik written advice on the need to collect personal information, its storage, use and disclosure will be provided to the client. Such advice will include information required by the client to access their record for the purpose of ensuring its accuracy and correction if necessary.
8. Where, in the course of providing services to clients, information is recorded such as clinical notes, plans, charts, records of diagnostic tests, records of treatment and medication such information is to be recorded accurately and only in prescribed files. Only information relevant to the needs of the client is to be recorded.

Collection of personal information from third parties

1. Where information is obtained from a third party or, for whatever reason, required personal information cannot be obtained directly from the client, persons who are requested to provide information on behalf of the client are to be identified, particularly where the person is a responsible person for the individual, and a record, including contact details, kept of the circumstances of their attendance and the information obtained.
2. Where possible, as soon as is reasonably practicable after the collection of information from third parties, including a person responsible, the privacy officer or a person delegated by the privacy officer to perform the task shall refer all information provided to the client for verification of its accuracy and completeness.
3. Staff should remain mindful that personal information, in particular sensitive information including health information, required to be collected may not be known to the third party being requested to provide information. Third parties, including a responsible person, should not be requested to confirm such information previously obtained except where consent to discuss such information with the third party is recorded on the file or in the case of a serious threat to the health or welfare of the client.

Use and disclosure of information

Boandik will not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose unless:-

1. The secondary purpose is directly related to the primary purpose and the person could reasonably expect the organisation to use or disclose the information for the secondary purpose.
2. The individual has consented to the use and disclosure.
3. Health information is to be used for research or compilation of statistics relevant to public health or safety and it is not practical to obtain the individual's consent. In these situations the use or disclosure must be conducted in accordance with the National Privacy Principles and Boandik must be sure that the information will not be disclosed to others or personal information derived from the health information.
4. A permitted general situation exists.
5. A permitted health situation exists.
6. The information is required to comply with legislative requirements including the Australian Privacy Principles and the SA Government Information Sharing Guidelines.

Boandik can disclose health information about a client to a person who is responsible for the client if:-

1. The client is physically or legally incapable of providing consent or
2. Physically cannot communicate consent or
3. The disclosure is necessary to provide appropriate care or treatment or
4. The disclosure is made for compassionate reasons.

In all of the above circumstances the disclosure must not be contrary to any wish expressed by the client.

Retention of information

1. As a general rule all information collected by Boandik for use in providing a service to its clients will be retained by Boandik for seven (7) years following the date of the last service provided to the client. Records for clients who are aboriginal will be retained indefinitely.
2. Personal Information collected which is not relevant to the services requested will not be retained but shall be destroyed as soon as practicable after collection.
3. At the time any file maintained by Boandik is considered to be finalised such files are to be referred to the privacy officer for a determination of the period the file is to be retained.

The retention period of any file is to be recorded by the privacy officer on the outside of the file.

Health records of adult clients are to be maintained for a minimum of seven (7) years following the date of the last recorded service provided to the adult client.

Verification of information

1. As soon as possible after the collection of personal information a copy of the recorded information provided by the client or third party is to be given to them for review to ensure that the information recorded is correct.
2. Processes will be established to ensure Boandik is advised of changes to client information.
3. On each occasion a client returns to Boandik, any existing records are to be retrieved and verified against any further information received to ensure all records are accurate, complete and up-to-date.
4. Except in the circumstances outlined in "collection of information from third parties" no review of information held by Boandik will be undertaken with a third party without the specific authorisation, in writing, of the individual.
5. An individual may, at any time, request access to information held by them for the purpose of verifying the information held (see minor requests below).

Contact process

Staff of Boandik may often have cause to contact persons about their record. In such situations the fact that a record has been collected may be revealed to a third party leading to a breach of privacy. This may occur when making follow up calls to check on a client's progress or in submitting accounts to the client on organisation letterhead.

(a) If specifically requested contact with a client by mail will not be sent in labelled envelopes. All staff collecting information will ensure that clients are advised of the usual procedure in sending mail in labelled envelopes.

(b) Staff contacting the client by telephone shall identify the client before identifying Boandik in any telephone contact so as to ensure the client's privacy is not compromised. Messages should not be left on answering machines or with third parties without the consent of the client.

Security of information

1. Only staff specifically authorised or required to use or refer to it may have access to any personal information in respect of clients held by Boandik. Any unauthorised disclosure or use of personal information by staff will result in disciplinary action which may include instant dismissal from employment.
2. All personal information held by Boandik which may contain any sensitive information will be secured. If in electronic form it will be protected by password only known to relevant staff, if in written format it will be in lockable filing cabinets or similar facilities. Where this is not practicable, for example where access is required continually, all records used in such circumstances are to be maintained under the constant supervision of a responsible staff member and access limited to persons requiring access to the record for the provision of services by Boandik.
3. Files may be taken out of the office for review with a client, by staff that work from home or at a different part of the organisation. The files will be transported in a locked bag as per the relevant procedures.
4. Sensitive information retained in safe storage will be removed from such safe storage only for the use of staff members tending to the provision of services to the client or for other legitimate reference.
5. Equipment used for transfer of information has appropriate security measure in place. Facsimile machines are located in an area that is lockable with access only available to authorised staff.
6. The privacy officer will be consulted prior to any personal information held on files being copied or disclosed to third parties. The privacy officer will determine whether the written consent of the client is required before personal information can be released. Copies of information made in accord with this policy are to be treated as if they were original records.
7. Any breach by staff of items 2 to 4 above may result in disciplinary action being taken by Boandik.
8. Boandik will act promptly and proactively if a data breach occurs in accordance with the data breach response proactive.
9. A data breach must be reported to the department head immediately staff are aware of the breach.

Destruction of information

1. All personal information no longer required which is in written or paper form is to be destroyed by means of confidential shredding, pulping, burning or disintegration of the written documents. This will occur seven years from the last service provided to a client other than aboriginal clients whose records will be kept indefinitely.
2. Electronic records will be deleted from databases at the same time as the destruction of written or paper documents
3. A suitable contractor who provides a guarantee of secure destruction may be engaged to dispose of information held in written or paper form. A certificate is to be requested from such contractor confirming destruction of the said records.
4. Electronic records are to be overwritten before deletion. All electronic data storage devices, including back up devices, are to be audited at least once every 18 months to ensure no non-essential data is retained in electronic form.
5. All discs, including hard drives, are to be degaussed prior to sale or disposal so as to ensure no electronic date continues to be stored thereon.
6. A register is to be maintained with details of all files destroyed which includes CIM number, name, Boandik service, date of entry, date of departure and date file was destroyed.

Openness

1. Boandik is bound by this policy to comply with the Australian Privacy Principles and all staff of Boandik shall comply with such principles and respect the rights of clients to privacy and access to their records.
2. All persons providing personal information to Boandik shall be provided with written advice on the reasons for the collection of the personal information, the purpose for which the information is to be used and the person's rights of access to and, if necessary, correction of, any information held by Boandik.
3. Staff are authorised to and shall, on request of any person, advise that person in general terms of the kind of personal information held by Boandik as follows:
    - Medical records;
    - Nursing notes;
    - Pharmacy records;
    - Address details;
    - Emergency contact details including names of next of kin.
4. Any persons requesting access to personal information held by Boandik shall be advised of the requirements of Boandik's access policy.
5. Clients will receive an annual reminder in newsletters of the privacy policy, confidentiality requirements and their ability to request access to records.

Access to records

1. On all occasions on which personal information is collected, the client or the person from whom the personal information is collected will be shown the original record or be provided with a copy of the personal information collected for the purpose of verifying the accuracy of the information recorded.
2. The client has the right to decide the personal information that is provided to an external person or authority. However there are certain circumstances where this can be overridden, including when:-
3. There is an obligation not to conceal a crime or intended crime
4. Disclosure may be required in the person's interest, eg allegations of abuse
5. In these situations the department head will consult with the privacy officer before information is released. The release of this information will be recorded in the register.
6. With the exception of minor requests for Information (see below) as a general rule persons requesting access to information held by Boandik will be asked to put their request in writing identifying themselves and their contact details and stating the information required.
7. Upon receipt of a request for access to information the privacy officer will undertake all reasonable steps to ensure the identity of the person requesting the information and, if the person is a responsible person, confirm that person's identity and status as a responsible person.
8. On satisfying themselves as to the identity and status of the party requesting access the privacy officer will enter details of the request into a record maintained for the purpose of recording requests for access, record the details of the person requesting the information and any subsequent action in respect of each request.
9. The privacy officer will assess all requests for access to personal information to determine that no information requested or for which release is proposed identifies or impacts upon the privacy of any other person. In such case any information which tends to identify another person will be deleted prior to release.
10. Prior to release of information to an individual the privacy officer may, if deemed by them to be appropriate and if acceptable to the person requesting the information, arrange an opportunity to discuss the information to be provided in order that the information may be properly understood and is not taken out of context particularly where such information may be distressful to the individual concerned.

11. Information will not be released if the release of such information is likely to endanger the life, health or safety of any individual, including the person requesting the information and the person about whom release of the information is sought.
12. Information of a commercial nature will not be released unless management of Boandik approves such release.
13. Boandik will not, except on advice from competent legal counsel, release personal information under this policy if the purpose of the request is to obtain information in respect of Boandik which may be used against Boandik in legal proceedings and is not otherwise discoverable in pre-trial proceedings.
14. The privacy officer may refrain from responding to a request for release of or access to personal information if, in the opinion of the privacy officer after consultation with the chief executive officer/department head such request is frivolous or vexatious. The privacy officer will maintain a record of all such requests and their reasons for refusing release.
15. Information, the release of which is prevented by law or release of which is likely to prejudice lawful enquiries, will not, following consultation with the policing authority, be released without authority.
16. Where a request for the release of information is refused the privacy officer will (unless requested to withhold the information by a law enforcement body) advise the person requesting release of the information the reason for the refusal to release the information sought and the avenues of appeal available to them.
17. Where possible receipt of a request for release of or access to personal information will be acknowledged immediately and the information requested provided to the person requesting it within 14 days of receipt of the initial request.
18. Information provided in response to an application may, if requested by the person, be transmitted by facsimile or electronic means only if the privacy officer is satisfied that the information to be provided will be received in a secure environment.
19. Where possible information will be personally delivered to the person requesting the information. Where delivery by mail is requested information will be posted by registered mail at the cost of the person requesting the information.
20. Information will be provided to third parties, eg legal representatives, only on receipt of a signed authority from the person in respect of whom the information is held. The original of such authorities will be retained by the privacy officer and a copy placed on the client file with a record of the date and information provided.
21. Unless specifically instructed by the client to the contrary medical records may be passed to non-treating medical practitioners if considered to be a directly related secondary purpose for the care and welfare of the client for the purposes of obtaining specialist advice and/or opinions respecting the clients care and proposed medical procedures, tests and similar purposes.
22. Upon receipt of a request for release of or access to personal information the privacy officer will assess the request and the costs involved in providing the information. The privacy officer will, after estimating the cost, contact the person requesting access and advise them of the likely cost of providing the information requested. The person requesting access may then amend their request or confirm their request on the basis of the amount to be charged. The amount charged will not exceed the actual cost of providing the information requested.
23. If, upon provision of information, the person provided with the information advises of an error in the information provided the privacy officer will take written instructions of the nature and details of the error or errors reported and will append such written instructions to all documents which are or are likely to be affected by the error.
24. As a general rule original documents will not be provided in response to an application for access unless such are specifically requested. If original documents are requested the privacy officer will ascertain the need for such access and will obtain legal advice before releasing original documents.

Minor requests for access

1. A minor request for Information is made when a person seeks to view their record in person merely to check information readily available. The purpose of such access is to allow the person requesting access to verify information held.
2. A person may have access to their record if such records are readily available at the time of the request.
3. The staff member of whom the request has been made, upon establishing that the person requesting access is the person about whom the information has been recorded and that the person only wishes to view the information, shall allow the person access to the information.
4. Access granted in this manner will be supervised by a staff member and the record kept under control of the staff member at all times. The staff member may answer any questions asked by the individual and may explain the meaning and context of the information viewed.
5. Photocopies of a limited number of documents may be taken.
6. A record of such access will be recorded consisting of the date of the access, details on how the person's identity was established, a record of any copies of documents taken and any amendments advised.
7. Amendments should be advised and such advice recorded but no alteration to any documentation permitted.
8. Any questions in respect of minor requests must be referred to the privacy officer.

Cross-border disclosure

Boandik may provide information to a responsible person who lives outside Australia. The client will have provided permission to disclose the information to the responsible person or it will be a permitted health situation. There are no other circumstances that would require Boandik to provide information to an entity outside Australia.

Correction of records

1. Following a grant of access to a record, a person about whom personal information is held may request in writing that the personal information held be amended or corrected.
2. All requests to amend or correct personal information held are to be referred to the privacy officer, who will record details of the request in a register maintained for the purpose of recording requests for access.
3. The privacy officer on receipt of a request to amend or correct personal information will append to any original written record details of the correction requested in such a manner that the amendment is readily apparent as a correction.
4. At no time is a written record to be altered or the original record obscured, erased, cut out or otherwise made unreadable.
5. No subsequent use and/or disclosure of any written record is to occur without use and/or disclosure of the amendment.
6. In the case of electronic or other forms of data storage a new record will be made recording the date of effect as the date the correction or amendment was made and will be cross referenced to the original record in order that the original of the record may be accessed if required.

Identifiers

Boandik will assign each client, where necessary, a unique identifying cypher that may be used for reference within Boandik. This cypher shall bear no resemblance to any existing number used by any other organisation, government department or agency, eg social security number, Medicare number or tax file number.

Anonymity

1. Unless required by law or for the provision of services to the person, no personal information tending to identify the person will be requested or recorded by Boandik.
2. All persons attending Boandik are to be advised that information provided to Boandik may be given anonymously.
3. All persons attending Boandik are to be advised that while they have a right to remain anonymous certain information will be required and that services cannot be provided to them unless their identity is recorded used or disclosed.

Complaints

1. Any complaint, written or oral, respecting any privacy issue is to be referred immediately to the privacy officer who will record and investigate the details of the complaint and maintain a statistical record of the type of complaint, section involved, form of breach (if any) and other details relevant to ensure an accurate assessment of the operations of the Privacy Policy.
2. The complainant is to be contacted by the privacy officer immediately the complaint has been received or within 24 hours weekdays, the following Monday for complaints received on weekends, and such contact is to be recorded on the relevant file and will record the complainant's version of events and their expectations.
3. On being contacted by the privacy officer the complainant is to be advised of the privacy officer's role to investigate the complaint, procedures to be followed and advice on how to contact the privacy officer directly, if necessary, being given the privacy officer's contact number to enable follow up of the complaint.
4. The privacy officer must assure themselves of the identity of the complainant who should be asked to put their complaint in writing if this has not already been done.
5. The privacy officer will investigate the complaint and may question staff in respect of the matter, examine documentation and systems to identify any shortcomings in procedures and/or this policy and to satisfy themselves as to any action needed to prevent any further breach of privacy.
6. Upon completion of the Investigation the privacy officer will prepare a report to the Chief Executive Officer with any recommendations for changes of procedure, this policy, disciplinary action or any other matter considered relevant by the privacy officer.
7. Upon completion of the investigation the complainant is to be advised of the results and any corrective action to be taken. As considered appropriate by the privacy officer this report may be given in writing, by face to face contact or by telephone with a record of the advice given to the complainant and their response recorded on the file.
8. If the matter cannot be resolved following investigation the complainant is to be advised of their rights under the Privacy Act or any relevant code and a report prepared for the appropriate body.
9. All complaints are, at all times, to be handled in a respectful manner with due consideration to be given to the rights of the complainant.
10. In the event that a complainant behaves in a vexatious, unreasonable or disrespectful manner the privacy officer may, at their discretion, discontinue the investigation, but in such case must record their reasons for so doing on the relevant file.
11. In the event that the privacy officer finds a complaint to be frivolous or unfounded after investigation, this fact will be recorded on the relevant file including the reasons for reaching the belief that the complaint is frivolous.

12. The privacy officer will keep a record of all complaints received and provide a report on comments and complaints to the quality committee bi-monthly.

The privacy officer and the chief executive officer will monitor the statistics on complaints to ensure that recurring problems are effectively dealt with.

Policy review

The application of this policy will be monitored and reviewed by the privacy officer through the conduct of internal and external audits and monitoring of the complaints system. Internal systems audits will be conducted annually by the privacy officer and relevant employees. A report on the findings of such internal and external audits shall be provided to the board of directors.
To ensure compliance with privacy principles, relevant personnel will conduct annual inspections of Boandik's documentary security facilities and procedures including waste disposal and submit reports to the privacy officer who will submit a report to the board of directors on Boandik's compliance with this policy and the Australian Privacy Principles.

External audits could be conducted by:
1. Relevant statutory authorities
2. Privacy consultants approved by the board of directors
3. Industry bodies

Staff training

All new staff will be instructed in this policy and the importance of adhering to privacy principles in their initial induction training. Any changes to the policy will be advised to all staff. Adherence to this policy and the privacy principles is a fundamental term of each employee's contract of employment, a breach of which will lead to disciplinary action including, if warranted after investigation, dismissal from employment.

Outcomes

Risks to the privacy of clients and their records arising out of deliberate or inadvertent breaches of the Australian Privacy Principles will be identified, assessed and controlled.