Privacy and Security of Personal Health Information Policy

1. Context

Employees at Boab Health Services are committed to giving clients quality care and service. As part of this, we protect the privacy of clients and treat all client information including health information as private and confidential. Boab Health Services has developed and documented a Privacy and Security of Personal Health Information Policy and Procedure according to the current privacy laws. These policies and procedures describe how employees at Boab Health Services abide by the outlined governing principles and understand that a breach is grounds for dismissal.

2. Purpose

The Privacy and Security of Personal Health Information Policy and Procedure outlines how personal health information is managed by Boab Health Services. It also includes the steps an individual must take to obtain access to their health information.

Boab Health Privacy Policy States:

- What type of personal information we collect
- Purpose of collecting personal information
- How we collect and store information
- The need for consent to collect personal information
- The right of access to information held by Boab Health
- How to access personal information
- How to discuss concerns you have about how we handle personal information
- How to make a complaint about a possible privacy breach

3. Scope

This policy applies to all staff, students, contractors, and volunteers at Boab Health Services who obtain or view personal health information while working, whether for business or personal reasons. It applies no matter whether the health information use takes place on company premises, while travelling or at remote sites. Privacy and security of personal health information reflects the values of the company: integrity, compassion, inclusiveness, respect, collaboration and excellence.

Health information platforms include (but not limited to):

- MMEx
- Email
- Fax
- Meetings

4. Responsibilities

Maintaining the privacy and security of personal health information is the responsibility of all Boab Health Services' employees. In addition to this, the following people have key responsibilities:

- The CEO is ultimately responsible for ensuring that Boab Health Services upholds the privacy and security of personal health information and in line with the company's values.
- The Executive Manager Clinical Services is responsible for overseeing the privacy and security of health information policies and procedures, including implementation of.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

- The **Regional Manager** and **Leadership Team** is responsible to providing updates or changes to this policy to broader teams within the organisation.

5. Privacy and Security of Personal Information Policy

Boab Health Services is bound by the Federal Privacy Act (1988) and the Australian Privacy Principles. 'Personal health information' is a particular subset of personal information and can include any information collected to provide a health service.

This information includes medical details, family information, name, address, employment and other demographic data, past medical and social history, current health issues and future medical care, Medicare number, accounts details and any health information such as a medical or personal opinions about a person's health, disability, or health status.

It includes the formal medical record whether written or electronic and information held or recorded on any other medium e.g., letter, fax, or electronically or information conveyed verbally.

Our Security policies and procedures regarding the confidentiality of client health records and information are documented and our team is informed about these at induction and when updates, or changes occur.

The team can describe how we correctly identify our clients using 3 client identifiers; name, and date of birth, address, or gender to ascertain we have the correct client record before entering or actioning anything from that record.

For each client we have an individual electronic health record containing all clinical information held by our service relating to that client. Boab Health Services ensures the protection of all information contained therein. Our client health records can be accessed by an appropriate team member when required.

For more information visit the federal privacy commissioner's website at www.privacy.gov.au or go to the state health service commissioners at www.dhs.gov.au/privacy.

6. Privacy and Security of Personal Information Procedure

Staff and contractors associated with Boab Health Services have a responsibility to maintain the privacy of personal health information and related financial information. The privacy of information is every client's right.

The maintenance of privacy requires that any information regarding individual client's may not be disclosed either verbally or in writing in electronic form except for strictly authorised use within the client care context at the clinical service area or as legally directed.

There are no degrees of privacy. All client information must be considered private and confidential, even that which is seen or heard and therefore is not to be disclosed to family, friends, staff, or others without the client's approval. Some details about a person's medical history or other contextual information such as details of an appointment can identify them, even if no name is attached to the information. This is still considered health information and as such it must be protected under the Privacy Act.

Any information given to unauthorised personnel will result in disciplinary action and possible dismissal. Each staff member is bound by his or her privacy clause contained within the employment agreement which is signed upon commencement of employment at Boab Health Services.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

Personal health information should be kept where staff supervision is easily provided and kept out of sight of the public e.g. left exposed on the reception desk, in waiting room or other public areas; or left unattended in a consulting or treatment room.

Computers and servers have sound backup systems and a contingency plan to protect the service from loss of data. Care should be taken that the general public cannot see or access computer screens that display information about individuals. To minimise this risk, automatic screensavers are engaged.

Members of the practice team have different levels of access to client health information.

Reception and other staff should be aware that conversations in the main reception area can often be overheard in the waiting room and as such staff should avoid discussing confidential and sensitive client information in this area. Whenever sensitive documentation is discarded Boab Health Services uses an appropriate method of destruction, a locked confidential waste bin is stored on site.

7. Correspondence

Electronic personal and/or confidential information is transmitted over the public network in an encrypted format using secure messaging software (MMEx). Where medical information is sent by post, the use of registered postage or courier service is determined on a case-by-case basis. Incoming client correspondence is left in a secure area and not in view of the public.

8. Facsimile

Fax, printers and other electronic communication devices are located in areas that are only accessed by Boab Health Services staff. Faxing is point to point and will therefore only be transmitted to one location. All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver.

Keep the transmission report produced as evidence that the fax was sent. Confirm the correct fax number on the report. Boab Health Services uses a fax disclaimer notice on outgoing faxes that affiliates with the service: “if you are not the intended recipient of this fax, please return to the fax number above and shred”.

9. Emails

Emails are sent via various modes and are at risk of being intercepted. Client information may only be emailed if it is securely encrypted according to industry and best practice standard.

10. Client Consultations

Client privacy and confidentiality is maximised during consultations by closing consulting/treatment room doors. When consulting/treatment room doors are closed staff should knock and wait for a response.

Where locks are present on individual rooms these should not be engaged except when the room is not in use.

It is the health practitioner’s responsibility to ensure that any personal client information is kept secure if they leave the room during a consultation or whenever they are not in attendance in the consulting/treatment room.

11. Medical Records

The physical medical records and related information created and maintained for the continuing management of each client is the property of Boab Health Services. While the client does not have ownership of the record, he/she has the right to access under the provisions of the Commonwealth Privacy and state Health Records Acts. Requests for access to the medical record will be acted upon only if received in a written format.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

Identity checks will be carried out on any access to records requests to ensure the security of personal information. Identity checks will be 2 part and include the provision of photo identification, e.g. drivers licence/Medicare.

Boab Health Services client records can be accessed by an appropriate team member when required. All team members have personal passwords, which are known only to them. Both active and inactive client health records are kept and stored securely.

12. Computer Information Security

Boab Health Services has systems in place to protect the privacy, security, quality and integrity of the data held electronically. Staff are trained in computer use and our security policies and procedures are updated when changes occur. All clinical staff have access to a computer, to document clinical care and for medico legal reasons. Staff always log in under their own username and password to document the care activities they have undertaken.

Boab Health Services ensures that our practice computers and service comply with the standard required of a health service provider:

- Computers are only accessible via individual username and password
- Access to health records is permission based
- Servers are backed up and checked at frequent intervals, consistent with the business continuity plan
- Back up information is stored in a secure offsite environment
- Computers are protected by antivirus software that is installed and updated regularly
- Computers are protected by appropriate hardware/software firewalls
- We have a documented business continuity plan
- Electronic data transmission of client health information from our service is in a secure format

Boab Health Services reserves the right to check individual's computer system history as a precaution to fraud, workplace harassment or breaches of confidence by employees. Inappropriate use of the service computer systems or breaches of practice computer security will be fully investigated.

Boab Health Services has a sound backup system and a contingency plan to protect service information in the event of an adverse incident, such as a catastrophic system failure. This plan encompasses all critical areas of the service operation such as making appointments, billing and collecting client health information. This plan is tested on a regular basis to ensure back up protocols work properly and that the service can continue to operate in the event of a systems failure.

13. Privacy Policy

The Australian Privacy Principles require a service to have a clearly documented policy on the handling of personal information, including health information.

Boab Health Services has a privacy policy document that is available on the Boab Health Services website and to anyone who asks for it and clients are made aware of this. The collection statement informs clients about how the health information will be used including internally and externally and under which circumstances that Boab Health Services will consider disclosing client information and any law that requires a particular information to be collected.

Client consent to be sharing of client health information is always provided at the commencement of treatment and clients must be made aware of the collection statement when giving consent to share health information.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

Information used for the purposes of internal quality improvement of clinical audit activities will be considered directly related secondary purpose and we do not seek specific consent for the use of client health information; however, we include information about quality improvement and clinical audit activities in our privacy statement and consent forms.

14. Privacy Procedure

Our privacy policy is located on our website:

https://boabhealth.logiqc.com.au//graphql/downloadFile/fe5bc729-5919-46fd-88bf-474cfa1e6784?file=a17f5715-a112-4071-affc-ac3900c5b924&filename=200917%20doc_145_Privacy%20Policy_v3.docx

15. Third Party Requests for Access to Medical Records or Health Information

Requests for third party access to the health records should be initiated by either receipt of correspondence from a solicitor or government agency or by the client completing a request in writing to the Executive Manager Clinical Services.

During the consent to treatment process, it is vital that health care practitioners inform clients what could be done with their personal health information. This information should be provided both verbally and in writing.

If you have received information or reports from another organisation such as a medical specialist, you are required to provide access in the same manner as for the records that are created by Boab Health Services. If the specialist has written 'not to be disclosed to a third party' or "confidential" on their report, this has no legal effect in relation to requests for access under the Health Records Act. You are required to provide access to records which have been transferred to you from another health service provider.

Boab Health Services only transfers client information to a third party once the consent to share information has been signed. Written request for access to records should be scanned into a client's medical record. All requests for access to medical records should be forwarded to the Executive Manager Clinical Services.

Records must be reviewed by the treating health professional prior to release to a third party. Boab Health Services retains a record of all requests for access to medical information including transfers to other services. These are scanned into the client's record. Requests for access to notes are tracked and monitored via the Access by Third Party Records Register.

16. Relatives and Friends

Clients may authorise another person to be given access if they have a legal right to sign authority.

In 2018 the Australian law reform commission recognised that the disclosure of information to a person responsible for an individual can occur within current privacy law. If a situation arises where a request to access records is received from a third party relative or friend this should be referred to the Executive Manager Clinical Services before such access is granted.

Care and consideration should be given to the health records of children whose parents have separated. Care must be taken that sensitive demographic information relating to either parent is not recorded on the demographic sheet. Significant court orders relating to custody and guardianship should be recorded on the children's records.

17. External Doctors and Healthcare Institutions

Any requests to be directed to the Executive Manager Clinical Services.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

18. Police and Solicitors
Police and solicitors must obtain a case specific signed client consent or subpoena/court order or search warrant for release of information. The request should be directed to the Executive Manager Clinical Services.

19. Health Insurance Companies, Workers Compensation, Social Welfare Agencies
Depending on the specific circumstances, information may need to be provided. All requests to be directed to the Executive Manager Clinical Services.

20. Employers
If the client has signed a consent to release information for a pre-employment questionnaire or similar, then direct the request to the Executive Manager Clinical Services.

21. Government Agencies
Depending on the specific circumstance information may need to be provided. Direct request to Executive Manager Clinical Services.

22. Researchers & Quality Assurance Programs
Where the service seeks to participate in research activities and continuous quality improvement activities client anonymity must be protected. Boab Health Services will retain a copy of any client specific data collection for research purposes. Research requests must be approved by the CEO and must have approval from human research ethics committee (HREC) constituted under the NHMRC guidelines. A copy of the approval will be retained by Boab Health Services.

Service accreditations is recognised as a peer review process and the reviewing of medical records for accreditation purposes has been deemed as a "secondary purpose" by the office of the federal privacy commissioner. As a consequence, clients are not required to provide consent.

23. Media
Please direct all enquiries to the CEO. Staff must not release information unless it has been authorised.

24. Telephone Calls
Requests for client information must be treated with care and no information is to be given. All requests for information must be received in writing.

25. Clients request for access to personal health information under privacy legislation policy
Clients have the right to access the personal health information under legislation. The Health Records Act gives individuals a right of access to the personal information held by any organisation in the private sector in accordance with Australian Privacy Principle 12. This principal obliges health service providers and other organisations that hold health information about a person to get that access to the health information on request.

Boab Health Services' Privacy Policy sets out how we manage health information and the steps an individual must take to obtain access to their health information.

26. Reports by specialists
This information forms part of the client's medical record, hence access is permitted under the privacy laws.

27. Diagnostic results

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

This information forms part of the client's medical record, hence access is permitted under privacy laws.

28. Release of Information Procedure

Clients are provided with information related to the right to access health information and of our commitment to privacy legislation compliance. Release of information will only occur in accordance with the privacy laws.

Request received

When a client requests access to medical records and related personal information held by Boab Health Services, we document each request and assist clients in granting access where possible and in accordance with the privacy legislation. Exemptions to access will be noted and each client or legally nominated representative will be their identification checked prior to access being granted.

All requests to access records must be made in writing and forwarded to the Executive Manager Clinical Services.

Request by another (non-client)

An individual may authorise another person to be given access, if they have the right e.g. a guardian and if they have a signed authority. Under APP12 Access to personal information, a person responsible for the client, including a partner, family member, care guardian may apply to be given access. Identification and authority must be checked prior to access being granted.

Children

When a young person is capable of making their own decision regarding their privacy, they should be allowed to do so according to federal privacy commissioners privacy guidelines. Each case must be subject to the individual circumstances. However, Boab Health Services guides treating practitioners to seek parental consent for children under the age of 18. Note: A parent does not necessarily the right to their child's information.

Deceased Persons

A request for access may be allowed for deceased client's legal representative if the client has been deceased for 30 years or less and all other privacy law requirements have been met. Access remains contingent upon records still being available.

Acknowledgment of requests to access records

Each request is acknowledged in writing to the client confirming a request has been received. The letter of acknowledgement should be sent within 14 days as recommended by the National privacy commissioner.

Collate and Access information

Arrange for the treating health practitioner to review the health records. Refer to the access to records request to help identify what information is to be given to the client. Data may be withheld under privacy principles APP11 access and correction under APP 13 for the following reasons.

- Where access would pose a serious threat to the life of health of an individual.
- Where the privacy of other may be affected
- If a request is frivolous or vexatious
- If information relates to existing or anticipated legal proceedings
- If access would prejudice negotiations with the individual
- If access would be unlawful
- Where denying access is required or authorised by law

Access Denied

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

Reasons for denied access must be given to the client/requestor in writing.

Provide Access

Health information may be accessed in the following ways:

- View and inspect information
- View and inspect information with a health practitioner
- Take notes
- Talk with treating practitioner
- Obtain a copy of records

Check identity of Client/Requestor

- Ensure a visible form of ID is presented by the person seeking access eg drivers license, passport or other photo ID. Note the details of ID
- Does the person have the authority to gain access? Check age, legal guardian status, is the person an authorised representative

If the client is viewing the data, supervise each viewing so the client is not disturbed, and no data goes missing. If a copy of the record is to be given to the client, ensure all pages are checked and this is noted. If the treating health practitioner is to explain the contents to the client, ensure an appropriate time is made. Where possible the treating clinician will be informed and available to discuss the health record contents.

Requests to Correct Information

A client may ask to have their personal health information amended if he/she considers that is not up to date, accurate and complete (APP 13).

Boab Health Services will try to correct the information if deemed appropriate. Where there is a disagreement about whether the information is indeed correct, Boab Health will attach a statement to the records outlining the client's claims.

Time Frames

All requests for access must be acknowledged within 14 days.
All requests must be completed within 30 days.

Privacy Audit

Periodically or in the event of any issues or complaints relating to privacy matters, Boab Health Services conducts a review of privacy policies and procedures.

Backup of Electronic Medical Records

To avoid lengthy down time, disruption and medico-legal issues frequent backups are essential and form a critical component of the service business continuity plan. A formal policy for the backup of the service computer system is in place.

Retention of Records and Archiving

- Child Clients - health records must be kept until the client is 25 years of age
- Adult Clients – health records must be kept for a minimum 7 years (for Aboriginal and Torres Strait Islanders, client records are kept indefinitely)
- Inactive electronic client records are retained indefinitely. Client records are marked as inactive.
- Client accounts records are retained for a minimum of 7 years.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.

- The service has a process in place to allow for the timely identification of records.

Transfer/Sharing of Medical Records

Transfer of medical records from this service can occur in the following circumstances:

- For medico-legal purposes eg record is subpoenaed to court
- When a client requests and consents to their medical record being transferred/shared with another service provider

Receiving a request to transfer/share medical records to another service

In accordance with state and federal privacy regulations a request to transfer medical records must be signed by the client giving us authority to transfer their records. Sharing of health records consent is outlined in the client treatment consent form. All reasonable steps are taken to protect the health information from loss and unauthorised disclosure during the transfer.

© This document is the property of Boab Health Services
Once printed this document is considered an uncontrolled version. Refer to the BHS LOGIQC QMS for the current approved version.