



THE HADER CLINIC
Corporate Policy

Privacy Policy

Creation Date	15/07/2026
Document Number	PL22731 V2
Owner	Jo Tyson
Contributors(s)	
Review Schedule	Three Years
Risk Rating	Medium
Effective Date	06/08/2026
Review Date	06/08/2029
Departments	Geelong
Standards	Standard 1 Goverance, Leadership Culture Standard 1 Patient Safety and Quality Systems Standard 6 Communication of critical information Standard 6 Documentation of information
Key Search Words	privacy, confidentiality, APP, breach, complaints, HCC

1 Policy Statement

The Hader Clinic is committed to protecting the privacy, confidentiality and security of all clients, employee and organisational information. All staff, volunteers, students, contractors and consultants are required to comply with relevant privacy legislation, maintain confidentiality and ensure personal, and health information is collected, used, stored and disclosed appropriately.

2 Policy Rationale

The purpose of this policy is to ensure compliance with the Health Records Act 2001 (Vic), support person-centred care, maintain trust with clients and residents, and provide guidance for the management of personal and health information.

3 Policy Scope

This policy applies to all staff, volunteers, students, contractors and consultants.

This policy covers, but is not limited to:

- Electronic records
- Paper records
- Verbal communication
- Emails
- Text messages
- Photographs
- CCTV

4 Roles and Responsibilities

Related to this policy

4.1 Boards and Executives

- Ensure compliance with legislation
- Monitor privacy risks

4.2 Director of Nursing

- Manage immediate privacy and confidentiality breaches
- Investigate breaches and implement corrective actions
- Coordinate root cause analysis for serious breaches.
- Coordinate mandatory reporting requirements where applicable
- Escalate significant breaches to Clinical Board of Governance
- Review and update privacy-related policies and procedures as required.
- Liaise with regulators and external agencies when required.

4.3 Quality and Safety Manager

- Maintain oversight of privacy and confidentiality compliance.
- Support and participate in investigations of privacy and confidentiality breaches.
- Monitor trends and identify risks.
- Ensure privacy breaches are recorded within the organisation's incident management and risk systems.
- Monitor completion of corrective actions.
- Report privacy and confidentiality risks, incidents and trends to relevant governance committees.
- Facilitate privacy and confidentiality education and awareness activities.
- Review and update privacy-related policies and procedures as required.
- Liaise with regulators and external agencies when required

4.4 All staff, students, volunteers', contractors and consultants

- Maintain confidentiality
- Access information only when required
- Report breaches immediately

5 Definitions

Used in this policy and procedure

5.1 Confidentiality

Confidentiality refers to the obligation to ensure that any information or knowledge relating to the client is not shared with anyone not authorised to access it. Any information that a client provides about their health has been provided in confidence and should be kept confidential unless there is a compelling reason for it not to be. Discussions relating to clients must occur only in private clinical areas and with authorised individuals involved in care.

Whilst there is no specific confidentiality law in Australia, a person can sue for a breach of confidentiality if it can be shown that the breach resulted in damage or injury.

5.2 Confidentiality breach

A breach of confidentiality occurs when information that should have been confidential is disclosed to an unauthorised person.

5.2.1 Examples of confidentiality breaches

- Talking about clients in a public space.
- Recycling paper that contains personal client information.
- Leaving handover sheets in public areas.
- Giving information to a client's family without their consent.
- Talking about a client with another client.

5.3 Health information

Health information means information or an opinion about:

- an individual's physical, mental or psychological health, including any disability,
 - an individual's expressed wishes about the future provision of a health service
 - a health service an individual has received, or will be receiving,
- that is also personal information.

The personal information collected to provide a health service.

5.4 Privacy

In health care, privacy refers to a person's right to control how their personal and health information is collected, used, stored, and shared. Health professionals and healthcare organisations must keep a patient's information confidential and only access or disclose it when authorised or legally permitted.

5.5 Privacy Breach

A privacy breach (data breach) occurs when there is a misuse, unauthorised disclosure or loss of personal health information. Breaches of privacy can be accidental or intentional. Most breaches are

due to noncompliance with the Health Privacy Principles

5.5.1 Examples of a privacy breach

Sending an email with personal health information to the wrong recipient.

Not disposing personal health information correctly

Providing someone else's personal details such as a phone number without consent

5.6 Unauthorised access

Unauthorised access occurs when personal information is accessed by someone who is not permitted to do so.

5.6.1 Examples of unauthorised access

Looking up the record of a friend or family member

Accessing a clients record for personal use, such as to find a clients address or phone number.

6 Health Privacy Principles Victoria

The Health Records Act 2001 contains 11 Health Privacy Principles that regulate how personal health information should be handled by organisations. By law, all medical records and health information must be kept safe, secure and confidential.

6.1 Collection - only collect personal information that is necessary.

- 6.2 Use and Disclosure – only use or disclose information for the purpose it was collected, or a directly related secondary purpose where it could reasonably be expected that the information would be used or disclosed
- 6.3 Data Quality – ensure personal information is accurate, complete and up to date.
- 6.4 Data Security and Data Retention – take steps to ensure personal health information is protected from loss, misuse, unauthorised access, modification or disclosure
- 6.5 Openness – policies on how personal information is managed
- 6.6 Access and Correction – individuals have a right to access their personal health information and correct the information if required.
- 6.7 Identifiers – only assign a number to identify a person if this is reasonably necessary, sharing of unique identifiers must be limited..
- 6.8 Anonymity – provide the option for individuals to not identify themselves if it is lawful and feasible
- 6.9 Transborder Data Flows – only transfer information outside of Victoria if the laws regarding privacy are similar to those in Victoria.
- 6.10 Transfer or closure of the practice of a health service provider – must notify past services users if a business will be sold, shut down, or a change of ownership.
- 6.11 Making information available to another health service provider – health service providers must make information available to another health service provider if requested by an individual.

7 Policy and Procedure

Related to this policy

7.1 Collection of Information

- Collect information lawfully
- Explain why information is being collected

7.2 Access to health information

- Under the Victorian Health Records Act 2001, individuals have the right to access health information collected by a private sector organisation on or after 1 July 2002.

Access can be by:

- inspection of the health information
- print out of health information
- provision of an accurate summary of the health information if the individual and organisation both agree a summary is appropriate
- an opportunity to view the health record accompanied by an explanation of the information by the health provider

Under the Act, fees may be charged for granting access to health information where permitted.

7.2.1 Refusal of access to health information

The Health Records Act 2001 sets out provisions where access to parts of a record may be legitimately refused, taking into account that access may not be appropriate.

If a request to access information would constitute a serious threat to an individuals' life or health, the request for access to that part of the health information must be refused. An individual health service provider nominated by the individual must provide a second opinion about the decision to refuse access to the information.

7.3 Storage and security

To protect privacy and confidentiality, all staff must:

- Access client information only when required to perform their duties.
- Use their own unique username and password to access electronic systems.
- Never share passwords or logins with another person.
- Keep passwords secure and confidential and change them regularly
- Log out of computers and electronic systems when not in use.
- Lock computer screens when leaving computer unattended for any period of time
- Ensure client information is not visible to unauthorised persons on computer screens, mobile devices or printed documents.
- Store paper records securely and not leave client information unattended in public or shared areas.
- CCTV recordings must be stored securely and protected against unauthorised access, alteration, loss or disclosure.
- Access credentials for CCTV systems must be restricted to authorised personnel and must not be shared.
- Copies of CCTV footage created for investigations, complaints or legal matters must be stored securely and only retained for as long as required.

Immediately report any suspected unauthorised access, loss of information, or security breach to the Director of Nursing.

7.4 Email and Electronic Communication

- Do not send client information through personal email accounts.
- Only use approved organisational email systems.
- Verify the recipient details before sending emails
- Use secure transmission methods where available.
- Encrypt sensitive information when appropriate.
- Do not store client information on personal devices

If an email containing personal or health information is sent to the wrong recipient, staff must immediately:

- Attempt to recall or retract the email where the email system allows.
- Contact the unintended recipient and request deletion of the email and any attachments without opening, saving, forwarding or distributing the information.
- Notify the Director of Nursing immediately.
- Document the incident and participate in any privacy breach assessment or investigation.

7.5 Mobile Devices

- Use organisation-approved devices.
- Enable password or biometric security.
- Report lost or stolen devices immediately.
- Do not store client information on personal devices.

7.6 Closed Circuit Television (CCTV)

Closed Circuit Television (CCTV) systems may be used within The Hader Clinic to support the safety, security and wellbeing of clients, visitors, staff, contractors and organisational property. CCTV is not intended to replace appropriate supervision, clinical care or workplace monitoring processes.

- CCTV footage is collected for security and safety purposes.
- Access is restricted to authorised personnel.
- Footage will only be disclosed where authorised by law or organisational policy.
- Footage will be securely retained and destroyed according to retention requirements.

7.6.1 CCTV footage

CCTV footage may be collected in common areas, entrances, exits, car parks, external grounds and other approved locations where there is a legitimate safety, security or operational need.

CCTV cameras must not be installed in areas where individuals would reasonably expect complete privacy, including bathrooms, toilets, or client bedrooms.

Signage will be displayed to inform individuals that surveillance is occurring

7.6.2 Access to CCTV Footage

CCTV footage is confidential and must only be accessed by authorised personnel for legitimate organisational, safety, security, clinical risk, complaint management or investigative purposes.

Access to CCTV recordings must be restricted to individuals specifically authorised by the Program Director, Director of Nursing, Program Manager or delegated manager.

7.6.3 Use and Disclosure

- CCTV footage must only be used for the purpose for which it was collected, unless otherwise required or authorised by law.
- Footage may be disclosed to Victoria Police, regulatory bodies, insurers, legal representatives or other authorised agencies where required by law, court order, warrant, investigation or other lawful authority.
- Any disclosure of CCTV footage must be documented and managed in accordance with privacy and confidentiality requirements.

7.6.4 Breach management

Unauthorised access, use, copying, disclosure or distribution of CCTV footage may constitute a privacy and confidentiality breach and must be reported immediately to the Director of Nursing and managed in accordance with the Privacy and Confidentiality Breach Process

7.7 Photography and Social Media

- Written consent must be obtained from the client, or their legally authorised representative, before taking, using, storing, publishing or sharing any photograph, video, or image of the client. Consent must be stored in the client's electronic clinical record.
- Client photographs and images must only be used for the specific purpose for which consent was provided.
- Consent may be withdrawn by the client at any time, and the image must not be used further once consent is withdrawn.
- Staff must not post, share, transmit, or publish client photographs, videos, personal information, or health information on social media or personal electronic devices.
- Staff must not identify a client directly or indirectly through social media posts, photographs, comments, stories, or online discussions, regardless of whether the client's name is used.
- Client images must be stored securely and accessed only by authorised personnel.
- Any unauthorised use, disclosure, or sharing of client images may be considered a privacy and confidentiality breach and may result in disciplinary action.

7.8 Retention and Disposal

- Clinical records must be retained in accordance with the Health Records Act 2001 (Vic). Adult client records must be retained for a minimum of seven (7) years from the date of the last entry in the clinical record.
- Records relating to a client who was under 18 years of age at the time services were provided, must be retained until the client reaches 25 years of age.
- Records must be stored securely and disposed of in a manner that maintains privacy and confidentiality.
- Records must not be destroyed where there is an actual or anticipated complaint, investigation, coronial inquiry, legal proceeding or other regulatory matter until the matter has been finalised and all applicable retention requirements have been met.
- CCTV recordings will be retained in accordance with organisational requirements and any applicable legislative or regulatory obligations.
 - Where footage is required for an incident investigation, complaint, legal proceeding, coronial matter or regulatory review, it must be preserved until the matter is finalised and all retention requirements have been met.
 - CCTV footage that is no longer required must be securely destroyed or deleted in a manner that prevents unauthorised recovery.

8 Clients' rights

Clients have the right to:

- Access their information
- Request corrections
- Make privacy complaints
- Be informed how information is collected and used
- Withdraw consent where applicable

8.1 Client' complaint process

Clients are encouraged to raise privacy concerns with the organisation initially with the Director of Nursing, or in writing via the client feedback forms.

Complaints will be investigated promptly and outcomes communicated to the complainant.

9 Disclosing Information

Client consent for collection, use and disclosure of health information must be obtained and documented unless otherwise permitted or required by law.

There are some situations where client information can be released without it being considered a breach of

confidentiality:

- If the client has consented for their information to be shared
- When required by law
- When sharing information to members of the healthcare team for continuity of care
- If a client threatens to harm someone else
- Liaising with a substitute decision maker If someone is permanently or temporarily incapacitated
- To prevent or reduce a serious threat to public health or safety

All disclosures of information must be recorded in the clinical record.

10 Privacy and Confidentiality Breach - Process

- Immediate reporting to the Director of Nursing.
- Containment of breach.
- Risk assessment.
- Investigation.
- Documentation
- Notification to affected person.
- Notification to regulator (if required).
- Corrective actions.
- Review and monitor
- Maintain records of the breach investigation and corrective actions

Where a privacy breach involves an email sent to an incorrect recipient, immediate attempts must be made to recall the email, contain the disclosure and assess the potential risk of harm to affected individuals.

All privacy and confidentiality breaches must be recorded as an incident in the electronic incident reporting system.

11 Health Complaints Commissioner

Clients may lodge a complaint directly with the Health Complaints Commissioner if they are dissatisfied with the organisation's response to a privacy or confidentiality concern.

11.1 Health Complaints Commissioner

12 Breaches and Disciplinary Action

All staff, contractors, volunteers, consultants and students are responsible for protecting the privacy, confidentiality and security of client information. Failure to comply with information security requirements, including sharing passwords, leaving computer screens unlocked or unattended, accessing records without authorisation, or improperly disclosing information, may constitute a breach of privacy and confidentiality.

Any suspected or actual breach must be reported immediately to the Director of Nursing or designated manager. Breaches will be investigated in accordance with organisational policies and procedures and may result in corrective action, additional training, disciplinary action, termination of employment, and notification to relevant regulatory authorities where required.

13 Documentation

All documentation relating to privacy and confidentiality must be stored securely, retained in accordance with legislative and organisational requirements, and be accessible only to authorised personnel. Documentation must be complete, accurate and maintained in a manner that protects privacy and confidentiality

The following records must be maintained in accordance with organisational record management requirements:

- Client consent forms relating to the collection, use or disclosure of personal and health information.
- Requests for access to, or correction of, health information.
- Records of disclosures of personal or health information.
- Privacy and confidentiality complaints.
- Privacy and confidentiality breach reports and investigation records.
- Risk assessments relating to privacy breaches.
- Corrective action plans arising from privacy incidents.
- Staff privacy and confidentiality training records.
- Confidentiality agreements completed by staff, students, volunteers, contractors and consultants where applicable.
- Privacy audit reports and monitoring activities.
- Notifications provided to affected individuals or regulatory authorities in relation to privacy breaches.

13.1 Incident reports

All privacy and confidentiality breaches must be recorded as an incident in the electronic incident reporting system.

14 Staff Training

All staff must complete privacy and confidentiality training during orientation, and yearly thereafter via OneVault.

15 Legislation and Acts

The Health Records Act 2001 (Vic)
Health Privacy Principles Victoria
Privacy Act 1988 (Cth)

16 Related Policies and Procedures

Employee Code of Conduct
Open Disclosure Policy
Complaints Management Policy

17 References

Used in this policy

17.1 Department of Health

17.2 Department of Health

17.3 Health Complaints Commissioner

18 Document Control

Ver 1 2026.08.06