S8-HCP-002
Privacy and Confidentiality

Document Control

Version Number	Key Personnel	Date
1	Managing Director	09 Sep 24
2	Managing Director	08 April 2026

Privacy and Confidentiality

Policy Statement

Holistic Horizons accepts and abides by the National Privacy Principles to protect personal information set out in the Privacy Act 1988 (Cth) and amended by the Privacy and Data Protection Act 2014 (QLD) and other privacy laws. In so doing, all personal information collected by the organisation will be carefully protected to ensure the individual's privacy is maintained.

Scope:

In this context, the following are defined as:

An **Individual** is any client, representative of a client, employee, visiting health professional, or visitor to Holistic Horizons.

Holistic Horizons maintains that privacy and confidentiality can be maintained by:

- Collecting only the information required under State and Federal legislation to deliver the service;
- Ensuring openness and consultation with individuals concerning the information collected;
- Providing individuals with access to their health and other records;
- Ensuring anonymity, where possible, and when requested by the individual;
- Disclosing personal information to other parties only with the consent of the individual or where it is legally or ethically justified; and
- Ensuring secure storage of information.

1.0 Procedure

1.1. COLLECTION OF PERSONAL INFORMATION

1.1.1. Holistic Horizons will only collect the personal information required to comply with State and Federal legislation for the delivery and funding of the clients' care and lifestyle needs, the employment of staff, or as otherwise required to provide aged care services.

1.1.2. Individuals will provide their personal information or be made aware of and agree to access personal information from other sources.

1.1.3. Holistic Horizons will provide the individual with information regarding the purpose and use of the personal information required and who will have access to the information.

1.1.4. Individuals will be informed of their right to withhold information or provide information anonymously, if applicable.

1.1.5. Individuals will be informed of the complaint's mechanism should they wish to lodge a complaint about how Holistic Horizons manages their personal information.

1.2. PROTECTION OF PERSONAL INFORMATION

1.2.1. Individuals will be informed of Holistic Horizons' responsibilities concerning the protection of personal information through:
- Handbooks;
- Brochures;
- Contracts/service agreements; and
- Policies and procedures.

1.2.2. All employees and volunteers will be required, on commencement of service, to sign a Confidentiality Agreement.

1.2.3. Employees will provide no personal information over the telephone unless established that the caller has legitimate grounds to access information and can give proof of identity.

1.2.4. The Managing Director or the Home Care Manager are the only individuals authorised to divulge employee information, where it is legally and ethically justified. They may nominate another employee of Holistic Horizons to provide this information in their absence in particular circumstances.

1.2.5. No personal information about anyone except the name of the caller should be left on voicemail.

1.2.6. Personal information will not be sent by email.

1.2.7. Employees are advised to avoid having personal mail addressed to their place of work.

1.2.8. The Administrative Officer is the designated person who opens the mail. All mail will be date stamped on receipt prior to distribution.

1.2.9. Mail addressed:
i. To a client will only be opened by the client and/or person(s) responsible
ii. By title or position alone will be opened by the designated mail opener
iii. "Personal" or "confidential" will be opened only by the addressee
iv. By title or position only and marked "personal" or "confidential" will be opened by the person occupying that position or by the person acting in the position.
v. To Holistic Horizons will only be opened by the designated mail opener and forwarded to the Managing Director.

1.2.10. Personal information should not be copied unless it is essential to do so.

1.2.11. The anonymity of clients and/or employees will be maintained during case presentations, research activities, seminars, and conference presentations.

1.2.12. Fictitious data should be used for all training and demonstration purposes.

1.2.13. Consent will be obtained to utilise photographs, slides and other visual aids that identify individuals.
1.2.14. Personal information related to clients and/or employees will not be discussed in public areas or with individuals who are not directly involved with the client's care or the employee's supervision.
1.2.15. All paper-based clinical records pertaining to current clients will be securely stored in the designated offices. Access to electronic clinical records will be limited to appropriate individuals who have been issued with a secure password.
1.2.16. All paper-based employee records pertaining to current employees will be securely stored in the Managing Directors office. Access to electronic employee records will be limited to appropriate individuals who have been issued a secure password.
1.2.17. All non-clinical data (agreements, asset declarations etc.) will be stored separately to clinical records and held in the Managing Directors office and only accessed by the Clinical Director/ Managing Director, Home Care Manager, and the Administrative Team involved with client agreements and accounts.

1.3. MEDIA

1.3.1. No information regarding a client, employee, visiting health professional, service provider or Holistic Horizons will be disclosed to the media by an employee.
1.3.2. No information is to be provided by any staff member to the media, even if it is 'off the record'.
1.3.3. A short file note should be prepared by the Worker summarising the nature of any media inquiry and the information provided in response to any media inquiry and given to the Managing Director.
1.3.4. Requests from the media for information will be referred to the Managing Director, who will determine what information will be provided. The decision will be based on consideration of:
   a. Consent from the relevant parties;
   b. Possible legal implications; and
   c. Ramifications to relevant individual(s) and/or Holistic Horizons.

1.4. ACCESS TO RECORDS

1.4.1. Access to clinical records (paper-based and electronic) is restricted to healthcare personnel currently involved in the care, observation, assessment, diagnosis, professional advice and management of the client, and other circumstances as described under Protocol "Authorised Disclosure".
1.4.2. Individuals will be made aware of their right to access their internal records and the process for doing so.
1.4.3. Through written application to the Clinical Director/Managing Director of Holistic Horizons, individuals may request access to their clinical records. As soon as practicable on receipt of the application, the Clinical Director/Managing Director will make the clinical record available to the on-site and in the presence of the Home Care Manager to assist with interpretation of the record.
1.4.4. The Managing Director may refuse a request by an individual for access to their clinical record:
   a. If the medical practitioner in charge of the persons care advises that the request should be refused; and/or
   b. If the Clinical Director/Managing Director is satisfied that access by the client and/or person(s) responsible would be prejudicial to the client's physical or mental health.
1.4.5. The application to the Clinical Director/ Managing Director for the request to access the clinical record will be retained in the client's clinical record.
1.4.6. An individual is entitled to dissent from or add to the clinical record. Their comments will be attached, as an addendum, to the record, along with an explanation of the circumstances.
1.4.7. Access to employee records (paper-based and electronic) is restricted to the Managing Director and their representative and designated administrative staff involved in human resource management activities and other circumstances as described under Protocol "Authorised Disclosure".
1.4.8. An employee is entitled to access their records and to obtain a copy of any document therein. In these circumstances, access will be on-site and in the presence of the Managing Director.
1.4.9. An employee is entitled to dissent from or add to their employee record. The employee's comments will be attached, as an addendum, to the record, along with an explanation of the circumstances.
1.4.10. Client medical and care records and staff records must be retained for a minimum of seven (7) years. Destruction must then be first authorised by the Home Care Manager or equivalent in consultation with the Operational Team Leader.
1.4.11. Confidential information should be shredded before disposal for security purposes.

1.4.12. Where an external service provider destroys confidential records, an agreement will be entered into by both parties.

1.5. AUTHORISED DISCLOSURE

1.5.1. Personal information regarding a client or employee may be disclosed:
   a. When valid informed consent is obtained from the individual for disclosure of specific information for a particular purpose;
   b. When an employee believes disclosure is necessary for the interests of public safety. In this situation, the employee should contact the Managing Director or their representative; and
   c. Where there is an obligation under the *Crimes Act* 1914 to notify police about serious criminal offences (including drug trafficking, serious assaults or murder and manslaughter).

1.5.2. Information will be provided to government authorities who have specific statutory powers to demand access to information. In these circumstances, the Managing Director will be responsible for responding to the subpoena promptly and will:
   a. Obtain the precise authority of the person requesting access, including reference to the Section of the Act under which access is authorised;
   b. Obtain the nature of the access requested to ensure that only material relevant to the statutory demand is released; and
   c. Bring the subpoena to the attention of a legal expert.

1.5.3. This information will be recorded and stored in the client's, employee's or other relevant files.

1.5.4. The use and disclosure of health information for secondary purposes (For example, research or collection of data for government departments) will be in accordance with the Health Privacy Principles 10(1)(d) and 11(1)(d).

1.6. NOTIFICATION OF ELIGIBLE DATA BREACHES

1.6.1. An Eligible Data Breach happens if:
   a. There is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
   b. The access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

1.6.2. Holistic Horizons must notify the affected individual(s) or organisation(s) (affected individuals) and the Office of the Australian Information Commissioner (OAIC) if:
   a. There are reasonable grounds to believe that an eligible data breach has happened; or
   b. Holistic Horizons is directed to do so by the OAIC.

1.6.3. All Workers are responsible for reporting an actual or suspected data breach to the Home Care Manager or the Managing Director.

1.6.4. The Home Care Manager or supervisor is responsible for taking immediate steps as per the *Data Breach Response Plan (Annexure 1)*, including:

a. Recording the reported breach using Part 1 of the *Data Breach Report Form (Annexure 3);*
b. Taking immediate steps to contain the breach; and
c. Notifying the Managing Director.

1.6.5. The Managing Director or delegate is responsible for investigating, assessing and responding to the data breach following the *Data Breach Response Plan (Annexure 1),* including:

a. Completing the *Data Breach Matrix (Annexure 2)*;
b. Completing Part 2 of the *Data Breach Report Form (Annexure 3);* and
c. Determining whether the breach is required to be notified and ensuring the relevant parties are notified.

1.6.6. If Holistic Horizons is required to notify affected individuals of an *Eligible Data Breach,* Holistic Horizons will do so by using the *Template Notification Letter* To *Individuals At Risk (Annexure 4).* The notification to affected individuals will include:

a. Holistic Horizons' identity and contact details;
b. A description of the data breach;
c. The kinds of information concerned; and
d. Recommendations about the steps that individuals should take in response to the serious data breach.

1.6.7. There are several exceptions to notification that may apply depending on the circumstances. These include:

a. If compliance with the notification requirements would be inconsistent with another law of the Commonwealth that regulates the use or disclosure of information, Holistic Horizons will be exempt to the extent of the inconsistency;
b. If compliance would be inconsistent with another law of that kind prescribed in regulations under the Privacy Act;
c. If the notification requirements in the My Health Records Act 2012 apply, then Holistic Horizons will be exempt to avoid double notification;
d. If Holistic Horizons has taken remedial action following an *Eligible Data Breach* or potential *Eligible Data Breach* and a reasonable person would conclude that as a result of the remedial action, the unauthorised access or unauthorised disclosure of personal information (including unauthorised access or unauthorised disclosure following a loss of the information) is not likely to result in serious harm to the affected individuals, or remedial action has prevented a loss of information from leading to unauthorised access or disclosure;
e. If remedial action following access or disclosure would lead a reasonable person to conclude that only particular individuals within a broader group are not likely to be at risk of serious harm following the remedial action, then Holistic Horizons will not be required to

notify those particular individuals (but would still be required to notify the remainder of the individuals); and

f. Suppose the Commissioner has (at the request of Holistic Horizons or the Commissioner's own initiative) exempted Holistic Horizons from providing notification of an Eligible Data Breach because the Commissioner is satisfied that it is reasonable in the circumstances to do so. In that case, Holistic Horizons may be exempt altogether or for some time.

1.6.8. Staff who fail to comply with this *Data Breach Response Policy* may face disciplinary action and, in serious cases, termination of employment.

Regulations	References
Aged Care Quality Standards Charter of Aged Care Rights Aged Care Act 1997 Work Health and Safety Act 2011 User Rights Principles 2014 Accountability Principles 2014 Information Principles 2014 Quality of Care Principles 2014 Records Principles 2014	Aged Care Diversity Framework Standard 8 Organisational Governance Translating and Interpreting Service (TIS National). Home Care Packages Program Operational Manual: A Guide for Home Care Providers. Standards Australia 2004 – AS/ISO 15489 - Records Management Standards Australia 1999 - AS 2828 – Paper Based Healthcare Records Standards Australia 1995 - AS 4400 - Personal Privacy Protection in Health Care Information Systems Standards Australia 2009 – AS/NZS/ISO 31000 – Risk Management – Principles and Guidelines Provider Responsibilities Relating to Governance – Guidance for Approved Providers

Consumer Outcome	Organisation Statement	Standard 8 Requirements
I am confident the organisation is well run. I can partner in improving the delivery of care and services.	8 (2) The organisations' governing body is accountable for the delivery of safe and quality care and services.	8 (3) The organisation demonstrates the following: 8 (3) (a) Consumers are engaged in the development, delivery and evaluation of care and services and are supported in that engagement. 8 (3) (b) The organisation's governing body promotes a culture of safe, inclusive and quality care and services and is accountable for their delivery. 8 (3) (c) Effective organisation wide governance systems relating to the following: (i) information management (ii) continuous improvement (iii) financial governance (iv) workforce governance, including the assignment of clear responsibilities and accountabilities (v) regulatory compliance (vi) feedback and complaints 8 (3) (d) Effective risk management systems and practices, including but not limited to the following: (i) managing high-impact or high-prevalence risks associated with the care of consumers

		(ii) identifying and responding to abuse and neglect of consumers (iii) supporting consumers to live the best life they can (iv) managing and preventing incidents, including the use of an incident management system. 8 (3) (e) Where clinical care is provided – a clinical governance framework, including but not limited to the following: (i) antimicrobial stewardship (ii) minimising the use of restraint (iii) open disclosure.

1.1. Data Breach Response Plan- Annexure 1

1. Purpose
The purpose of this *Data Breach Response Plan* is to establish a systematic approach for identifying, responding to, and reporting data breaches affecting personal information at Holistic Horizons. This plan aims to ensure compliance with the Privacy Act 1988 (Cth), the Privacy and Data Protection Act 2014 (QLD), and other relevant privacy laws while protecting the privacy and confidentiality of individuals.

2. Scope
This plan applies to all employees, volunteers, contractors, and third-party service providers of Holistic Horizons who handle personal information. This plan covers all forms of personal information collected, used, and stored by the organisation.

3. Definitions
- Data Breach: An incident that results in unauthorised access to, unauthorised disclosure of, or loss of personal information.
- Eligible Data Breach: A data breach that is likely to result in serious harm to any individual to whom the information relates.
- Personal Information: Any information that can identify an individual, including but not limited to names, addresses, contact details, and health records.

4. Responsibilities
- All Employees: Responsible for reporting any actual or suspected data breach to the Home Care Manager or the Managing Director immediately.
- Home Care Manager/Supervisor: Responsible for the initial response to reported breaches, containment measures, and notifying the Managing Director.
- Managing Director or Delegate: Responsible for investigating and assessing the breach, completing required documentation, and determining notification obligations.

5. Data Breach Response Steps
5.1. Identification and Reporting
- Immediate Reporting: Any employee who suspects a data breach must report it immediately to the Managing Director.
- Initial Assessment: The Managing Director will conduct an initial assessment to determine whether the incident constitutes a data breach.

5.2. Containment
Immediate Action: Upon confirmation of a data breach, the Managing Director will take immediate steps to contain the breach, which may include:
- Stopping the unauthorised access or disclosure.
- Securing the affected systems and data.
- Limiting access to affected records.

5.3. Investigation
- Investigation Team: The Managing Director will appoint an investigation team to conduct a thorough investigation of the breach.
- Data Breach Matrix: Complete the *Data Breach Matrix (Annexure 2)* to assess the severity of the breach, identify the affected individuals, and determine the type of information involved.

5.4. Documentation
- *Data Breach Report Form*: Complete Part 1 of the *Data Breach Report Form (Annexure 3)* to document the details of the breach.
- Ongoing Documentation: Document all actions taken in response to the breach, including containment, investigation, and mitigation efforts.

5.5. Notification
- Determine Notification Requirements: Based on the investigation, the Managing Director will determine if the breach is an Eligible Data Breach and if notification is required.
- Notify Affected Individuals: If notification is required, use the *Template Notification Letter To Individuals At Risk (Annexure 4)* to inform affected individuals.

The notification will include:

1. Holistic Horizons' identity and contact details.
2. A description of the data breach.
3. The kinds of information involved.
4. Recommendations for steps individuals should take in response.

5.6. Reporting to Authorities

- OAIC Notification: If required, notify the Office of the Australian Information Commissioner (OAIC) of the Eligible Data Breach, including:

1. Details of the breach.
2. The number of individuals affected.
3. Steps taken to address the breach

6. Post-Incident Review

- Review and Evaluation: After managing the data breach, conduct a review to evaluate the effectiveness of the response and identify any areas for improvement.
- Update Policies: Revise policies and procedures as needed based on the findings from the review.

7. Training and Awareness

- Training Programs: Regular training for all employees on data protection, breach reporting procedures, and privacy obligations.
- Awareness Campaigns: Ongoing awareness campaigns to reinforce the importance of privacy and confidentiality.

This Data Breach Response Plan aligns with the Privacy and Confidentiality Policy and outlines a comprehensive approach to handle data breaches effectively, ensuring compliance with legal obligations and safeguarding personal information.

1.2. Data Breach Matrix (Annexure 2)

Breach Scenario	Description	Potential Impact	Immediate Response	Mitigation Strategies
Unauthorised Access	An employee accesses personal information without proper authorisation.	Breach of confidentiality, loss of trust, potential legal implications.	Notify the Home Care Manager, document the incident, and restrict access.	Implement strict access controls, conduct regular audits of access logs.
Unauthorised Disclosure	Personal information is inadvertently shared with unauthorised individuals (e.g., through email or conversation)	Risk of identity theft, legal repercussions, reputational damage.	Inform the affected individual(s), notify the Managing Director.	Provide training on information sharing, establish protocols for sensitive communications.
Loss of Personal Information	Physical documents containing personal information are lost or misplaced.	Risk of identity theft, violation of privacy laws.	Report to the Home Care Manager, initiate a search for the documents.	Secure storage for physical documents, conduct regular inventory checks.
Data Breach via Cyber Attack	A hacker gains access to the organisation's electronic records system.	Major loss of confidential data, significant legal ramifications.	Notify IT security team, contain the breach, and assess damage.	Enhance cybersecurity measures, conduct regular security training for staff.
Breach due to External Provider	A third-party service provider mishandles personal information (e.g., data breach on their end).	Potential exposure of client data, loss of trust in the organisation.	Notify the Managing Director, assess the extent of the breach.	Vet third-party vendors for security compliance, establish data protection agreements.
Accidental Email Sent to Wrong Recipient	An email containing personal information is sent to an unintended recipient.	Breach of confidentiality, potential legal issues.	Notify the recipient, request deletion of the email, and inform the Managing Director.	Implement double-check procedures for sensitive communications, use secure email services.
Insider Threat	An employee intentionally accesses or discloses personal information for malicious purposes.	Severe legal implications, risk of identity theft for clients/employees.	Notify the Home Care Manager, conduct an investigation.	Conduct background checks during hiring, provide training on ethics and privacy.
Physical Theft	Personal devices (laptops, phones) containing sensitive information are stolen.	Potential data exposure, legal consequences, reputational damage.	Report to authorities, notify the Managing Director, contain the breach.	Use encryption on all devices, implement remote wipe capabilities.

Inadequate Disposal of Records	Personal information is not properly shredded before disposal, leading to potential exposure.	Risk of identity theft, legal ramifications.	Report the incident, assess the impact, and notify affected individuals if necessary.	Establish clear disposal policies, train staff on secure disposal practices.
Client Rights Violation	Failure to uphold clients' rights regarding access to and correction of their personal data.	Erosion of trust, legal repercussions, potential loss of clients.	Notify the affected clients, assess the situation, and take corrective action.	Regularly train staff on client rights and data handling, implement a transparent complaint mechanism.
Cultural Sensitivity Breach	Personal information is mishandled or shared without considering cultural sensitivities.	Risk of alienation of clients, reputational damage, potential legal issues.	Assess the impact and notify affected clients, inform the Managing Director.	Train staff on cultural awareness, implement protocols to ensure sensitive handling of diverse client data.

- Each breach scenario requires careful assessment of its impact and the required response according to the policy.
- Regular training and updates to the policy and procedures should be conducted to ensure all staff are aware of their responsibilities and the importance of data protection.
- Incorporating a culture of privacy and security awareness is essential to minimise the risks of data breaches.

1.3. Data Breach Report Form - Annexure 3

This form is intended to capture essential information about any suspected or confirmed data breach.

Part 1: Breach Reporting

1. Date of Report:
2. Name of Person Reporting the Breach:
3. Position/Title:
4. Contact Information (Email/Phone):

1. Details of the Breach

5. Date and Time of the Breach:
6. Date and Time the Breach was Reported:
7. Description of the Breach:

   (Include details such as how the breach occurred, what information was involved, and any other relevant details.)

8. Type of Breach (check all that apply):
   [ ] Unauthorised access
   [ ] Unauthorised disclosure
   [ ] Loss of personal information
   [ ] Other (please specify): _____
9. Individuals Affected:
   (List all individuals whose information was affected, if known.)

2. Containment Measures

10. Immediate Actions Taken to Contain the Breach:
    (Describe the steps taken to limit the breach's impact and secure the information.)
11. Was the Breach Contained?
    [ ] Yes
    [ ] No
    [ ] In Progress

Part 2: Investigation and Notification

12. Name of the Investigating Officer/Manager:
13. Investigation Start Date:
14. Investigation Completion Date:
15. Findings of the Investigation:

(Summarise the outcomes of the investigation, including causes and impacts of the breach.)

16. Recommendations for Future Prevention:
    (Outline any steps that should be taken to prevent similar breaches in the future.)

17. Notification Requirements:
    Will affected individuals be notified?
    [ ] Yes
    [ ] No
    If yes, describe the notification plan:

18. Additional Comments:
    (Any other relevant information regarding the breach or the response process.)

19. Signature of Person Reporting the Breach:

20. Date of Signature:

Submission Instructions:
Please submit this completed form to the Home Care Manager or the Managing Director immediately after reporting a data breach.

1.4. Data Breach Report Form - Annexure 4

[Holistic Horizons Letterhead]

[Date]

[Recipient's Name]
[Recipient's Address]
[City, State, Post Code]

Dear [Recipient's Name],

Subject: Notification of Eligible Data Breach

I am writing to inform you about a recent incident that has resulted in a breach of your personal information held by Holistic Horizons.

Details of the Breach:
On [insert date of breach], we experienced [briefly describe the nature of the breach, e.g., unauthorised access to personal information, loss of data, etc.]. We believe this breach is an "Eligible Data Breach" as defined under the Privacy Act 1988.

Information Involved:
The personal information that may have been affected includes [list types of information concerned, e.g., your name, contact information, health records, etc.].

Steps to Take:
To protect your information and mitigate any potential impact, we recommend that you take the following steps:

1. Monitor Your Accounts Keep an eye on your bank statements, credit reports, and any other relevant accounts for suspicious activity.
2. Change Your Passwords: If your login details may have been compromised, please change your passwords immediately.
3. Report Suspicious Activity: If you notice any unauthorised transactions or activities, please report them to the appropriate authorities immediately.
4. Consider Identity Protection Services: You may wish to consider enrolling in a credit monitoring or identity protection service for added security.

Holistic Horizons' Commitment:
We take the protection of your personal information very seriously. We are actively investigating this incident and have implemented measures to enhance our data security practices to prevent such incidents in the future. We encourage you to contact us with any questions or concerns regarding this matter.

Contact Information:
Should you have any inquiries or require further information, please do not hesitate to reach out to:

[Your Name]
[Your Position]
Holistic Horizons
[Contact Phone Number]
[Contact Email Address]
[Address of Holistic Horizons]

We sincerely apologise for any distress this incident may cause and appreciate your understanding as we work to resolve this issue.

Thank you for your attention to this important matter.

Sincerely,

[Your Name]
[Your Position]
Holistic Horizons

Notes for Customisation:
- Ensure that the letterhead includes Holistic Horizons' branding.
- Replace placeholder text (e.g., [insert date of breach], [Recipient's Name], etc.) with actual data.
- Tailor the recommendations based on the nature of the breach and the type of information involved.