Privacy and Information Management Policy and Procedures

*Evina Connect refers to Directors and contractors.

Policy Overview
Evina Connect is committed to adhering to all relevant privacy and information management laws and regulations, ensuring the protection and confidentiality of personal data. This policy applies to all Directors and Contractors associated with Evina Connect.

Evina Connect will comply with the following legislative frameworks:

- **Disability Services Act 1993**
- **NDIS Practice Standards Provider Governance and Operational Management Module (Information Management)**
- **Standard 1 of the National Standards for Disability Services**
- **The South Australian Privacy Committee** – Managing privacy complaints related to state government agency adherence to Information Privacy Principles
- **Health and Community Services Complaints Commissioner** – Complaints related to government, private, and non-government health and community services

Evina Connect will handle, store, and manage information in compliance with the **Privacy Act 1988** and its associated regulations.

This includes having comprehensive systems in place for the secure collection, use, storage, disclosure, access, correction, and disposal of personal data.

Desired Outcomes

- Full compliance with legislative privacy requirements
- Assurance to all participants that their personal data is secure, confidential, and only used for the intended purposes.

Background Information
The **Privacy Act 1988** sets out the legal framework for managing personal information within the Australian private sector. The **Privacy Amendment Act 2012** updated the **Australian Privacy Principles (APPs)**, which came into effect in March 2014. This requires organisations to be transparent about how they protect personal data and communicate these practices to their participants.

The South Australian Privacy Committee and the Health and Community Services Complaints Commissioner govern the retention of personal health data.

EVINA CONNECT

Definitions

- **Personal Information**: Any information (or opinion) held that can identify an individual, either directly or indirectly.
- **Sensitive Information**: A specific category of personal information, such as details related to health, race, religion, sexual orientation, etc.

Procedures

Ensuring Privacy and Confidentiality Compliance for Contractors

1. The **Director**s will review the Privacy Policy annually and ensure all Contractors are familiar with their responsibilities to protect participant privacy.
2. Contractors will undergo an initial and annual training on privacy, confidentiality, and information management. This training will be logged in the **Human Resource Log**.
3. All Contractors, including those substituting during leave or illness, will sign an agreement covering confidentiality and security, along with a **Contractor Checklist** confirming their understanding. Contractors will provide 100 points of ID, an **NDIS Worker Screening Check**, and a current police clearance before starting. They will also review and sign all relevant company policies and procedures.
4. Participants will be informed that when backfilling for absences, their information may be shared with the substitute Contractor. This Contractor is bound by the same privacy agreements and will face dismissal for any breaches. Participants may request a service cancellation or opt-out of contact during this period.

Storing and Managing Participant Information

1. Participant data is kept in individual records and can include personal details, clinical notes, investigation results, communication from healthcare providers, and multimedia (photos, videos).
2. Only authorised Contractors will have access to the online case-management system.
3. Information stored electronically will be secured using password-protected files, multi-factor authentication, and other security protocols.
4. Physical documents will be stored securely in locked cabinets.
5. Records are maintained for seven years from the last discharge date. For participants under 18, information is retained until they turn 25 or seven years post-discharge, whichever is later.
6. All personal data will be securely destroyed by shredding paper records and deleting files from electronic systems when no longer required.
7. User access is controlled by passwords and automatic log-out systems for all devices holding sensitive participant data.

8. Information will only be shared with other Contractors working directly with the participant.
9. Email accounts and the case-management system (Halaxy) will be protected with two-factor authentication for all users.

Halaxy Online Case Management System
Halaxy is the software platform used for case management, and it adheres to Australian privacy standards. It stores participant information securely in Australia with bank-level encryption and multiple backups. Halaxy complies with privacy laws, including the **Privacy Act 1988**, and provides a robust security framework to protect participant data.

Halaxy Security Details:

- Halaxy is based in Melbourne and uses encrypted data storage within Australia.
- Further security information is available at: Halaxy Security
- For support: Call 1800 984 334 or email community@halaxy.com

Managing Participant Privacy and Consent

1. Privacy requirements are clearly outlined in the participant's **NDIS Service Agreement**.
2. The agreement includes four consents that must be reviewed with the participant (or their decision-maker) before services commence:
    - Consent to share and obtain information
    - Consent to receive services
    - Consent to participate in satisfaction surveys
    - Consent to participate in quality management activities
3. Participants are informed of the necessity to provide accurate, up-to-date information when using Evina Connect's services.
4. Personal information will not be shared with external parties without the participant's consent unless required by law.
5. Any required data sharing will be strictly confined to relevant professionals with a duty of confidentiality and a professional code of ethics.
6. Evina Connect will inform participants about situations where information might be shared without consent due to legal obligations.

Maintaining Accurate Information

1. Participants must provide accurate and complete information. Evina Connect updates participant records at regular intervals, such as during service reviews, and whenever changes occur.
2. Evina Connect ensures participant information is updated promptly after services are delivered.

Using Participant Information for Other Purposes

Evina Connect will never use participant data for purposes beyond those outlined in this policy unless explicit written consent is obtained from the participant.

Participant Access to Their Information

Participants are entitled to request access to the personal data Evina Connect holds about them. They can do so by contacting the **Director** directly.

Handling Privacy Complaints

1. In case of a privacy complaint, the participant should first contact the Contractor involved and then the Directors. The complaint will be processed in accordance with Evina Connect's **Feedback and Complaints Management Policy**.
2. If the complaint is not resolved through internal channels, the participant may escalate the matter to an independent body, such as the **Office of the Australian Privacy Commissioner** or the **NDIS Quality and Safeguards Commission**.

Managing Data Breaches

1. If a data breach is suspected, the following actions will be taken:
    - The Contractor will complete a **Data Breach Form** and report the issue to the Directors.
    - The Directors will document the breach, including who's data was affected and the nature of the incident.
    - Affected participants will be informed of the breach and any disclosed information.
    - Evina Connect will report the breach to the **NDIS Fraud Line** and the **Office of the Australian Information Commissioner** via their website.
2. Evina Connect will work with the participant's Plan Managers to address any potential concerns regarding suspicious communications.
3. A review of the breach's cause will be conducted, and strategies will be implemented to minimise the risk of recurrence (e.g., staff training on identifying phishing emails).

Steps to Minimise Data Breaches

1. Weekly file backups to a secure external drive and encrypted cloud storage.
2. All paper records are stored in locked cabinets.
3. Email security includes two-factor authentication and an enhanced spam filter with the Australian-based provider, **VentraIP**.
4. Where possible contractors' devices are protected by VPNs, anti-virus, and malware software.

Website Data Security

Personal information provided via Evina Connect's website (such as email addresses, phone numbers, and resumes) is sent directly to the Directors and protected by **two-factor authentication**. Email security is provided by **VentralP**, an Australian-based email provider.

Reference

- 'Guidelines on Privacy in the Private Health Sector', Office of the Australian Information Commissioner

EVINA CONNECT

Appendix 1: Summary of the 13 Australian Privacy Principles

APP 1 — Open and transparent management of personal information
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive 'information.

APP 4 — Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.