healthylivingNT

Privacy Breach and Complaint Policy and Procedures

Policy Statement

Healthy Living NT (HLNT) is committed to maintaining client, member and customer privacy and confidentiality in accordance with HLNT's *Privacy Policy*. Healthy Living NT makes every effort to resolve a potential or actual breach of privacy, and complaints related thereto, originating from our role in providing assistance and services to members, clients and consumers.

Potential and actual breaches of privacy, and related complaints, are to be managed via this *Privacy Breach and Complaints Procedure*.

Definitions

APPs	mean the Australian Privacy Principles adopted in 2014
Complaint	is any issues of concern raised about a potential or actual breach of privacy during the course of administering and managing HLNT business
Complainant	means the person or organisation raising the complaint
Employees	refer to all staff, consultants, contractors and volunteers engaged in administration and management of HLNT business
Natural Justice	means applying a fair process without bias
Eligible data breach	A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the personal or sensitive information relates.
External Funder	means contracted services that HLNT hold with a variety of funders including (but not limited to) the OHS Agreement with the PHN, Service Agreements with NT DoH and the NDSS Agency Agreement with DAL
Personal and sensitive information	refers to any information of a personal and/or sensitive nature, for example contact details and a medical diagnosis, that identifies or could identify a person
Privacy	refers to how personal and sensitive information is handled
Privacy Act	means the Privacy Act 1988
Privacy breach	means when personal and/or sensitive information held by Healthy Living NT is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference
Privacy breach - potential	Means the circumstances, environment or work practices that could give rise to a privacy breach
Privacy Officer	is the HLNT CEO or in his/her absence the Manager Education Services
Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)	Establishes a Notifiable Data Breaches (NDB) scheme in Australia.The NDB scheme requires organisations covered by the Australian Privacy Act 1988 (Privacy Act) to notify any individuals likely to be at risk of serious harm by a data breach.

Policy

Life. Be in it.™

Scope

During the course of administering its business, Healthy Living NT collects and handles personal and sensitive information about a range of clients and members.

HLNT has implemented measures to ensure it meets contractual obligations and statutory and regulatory requirements including those mandated by the Privacy Act and the APPs.

The scope of this policy relates to identifying, recording, monitoring and resolving a potential or actual breach of personal and sensitive information, managing and resolving related complaints, and the action taken to prevent re-occurrences.

Objective

The objective of this policy is to ensure all potential or actual breaches of privacy, and complaints relating thereto, arising from the administration Healthy Living NT business:

- are comprehensively investigated in a timely manner
- have immediate corrective action applied
- are mitigated and resolved, applying the principles of natural justice, transparency and confidentiality to the satisfaction of the complainant and the person and/or the organisation against whom the complaint is raised
- is assessed, managed and notified consistent with statutory, regulatory and contractual obligations
- is recorded, reported and monitored according to continuous quality improvement principles, and
- have preventative actions applied to minimise risks of a repeat privacy breach.

Responsibility

It is the responsibility of all employees of Healthy Living NT to act in accordance with HLNT's Privacy Policy and use their best endeavours to act according to this Privacy Breach and Complaints Policy and Procedure.

Failure to act accordingly may result in mandated counselling, disciplinary action, or dismissal.

PROCEDURE

Step 1 – Containment and Preliminary Assessment

A privacy breach (potential or actual) may be identified in one of two ways:

a) a complaint by an external person or organisation or

b) a HLNT employee becoming aware of the breach, or the potential for a breach to occur.

External Complaint - Privacy Breach	HLNT Identified - Privacy Breach
The employee receiving the complaint: • records complainant's contact details and the preferred format for response e.g. verbal by phone or in person, by mail or email • acknowledges the nature of the complaint at time of complaint • assures the complainant that the complaint will be promptly investigated • informs complainant that an initial response will be provided within two (2) business days • records all details of the complaint, and	The employee identifying the breach: • records all details of the breach, • takes immediate action to eliminate further breach (where possible), and • refers the matter immediately to HLNT's Privacy Officer and their immediate supervisor for investigation and coordination. • Privacy Officer conducts preliminary assessment for determination of eligible data breach

• refers the complaint immediately to HLNT's Privacy Officer and their immediate supervisor for investigation and coordination. • Privacy Officer conducts preliminary assessment on determination of eligible data breach	

Step 2 – Risk Assessment

The Privacy Officer:

- takes immediate corrective action to eliminate further breach
- retains documentation of corrective action
- considers and identifies all potential harm caused by the breach
- notifies the complainant and/or affected individuals immediately if there is a high level of risk of serious harm
- formulates and forwards an initial response to the complainant within two (2) business days
- performs a risk analysis:
  - considering the type of personal and/or sensitive information involved
  - determining the context of the information and the incident
  - determining the extent and eligibility of data breach*

Step 3 – Notification

The Privacy Officer considers and determines external notifications to:

- funders such as DAL (NDSS) and NT PHN (MOICD) under the terms of the Service Agreement(s) and specific polices, and/or
- regulatory bodies such as police, financial institutions, insurers, professional or regulatory bodies and/or Office of Australian Information Commissioner.

Step 4 – Preventative Action

The Privacy Officer:

- documents privacy breach and/or complaint for record keeping, monitoring of re-occurrence and reporting purposes,
- investigates, determines and performs and/or delegates preventative action to minimise risks of similar privacy breaches, and
- implements any review of procedures in evaluation where linked with eligible data breach.

Step 5 – Privacy Breach Register

The Privacy Officer ensures that:

- full details of the breach or the potential breach are entered into a Privacy Breach Register and
- the register is submitted to the Board annually for review.

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

*Reference assessing eligible data breaches

https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme

Approval

Original Approval Date: Board Meeting 2/17 of 22 April 2017
Revision 1 Approval Date: Board Meeting 6/17 of 9 December 2017
Revision 2 Submission Date: Executive Board Meeting 1/18 of 1 March 2018
Revision 2 Approval Date: Executive Board Meeting 1/18 of 1 March 2018

Circulation: All HLNT Board Members and staff.

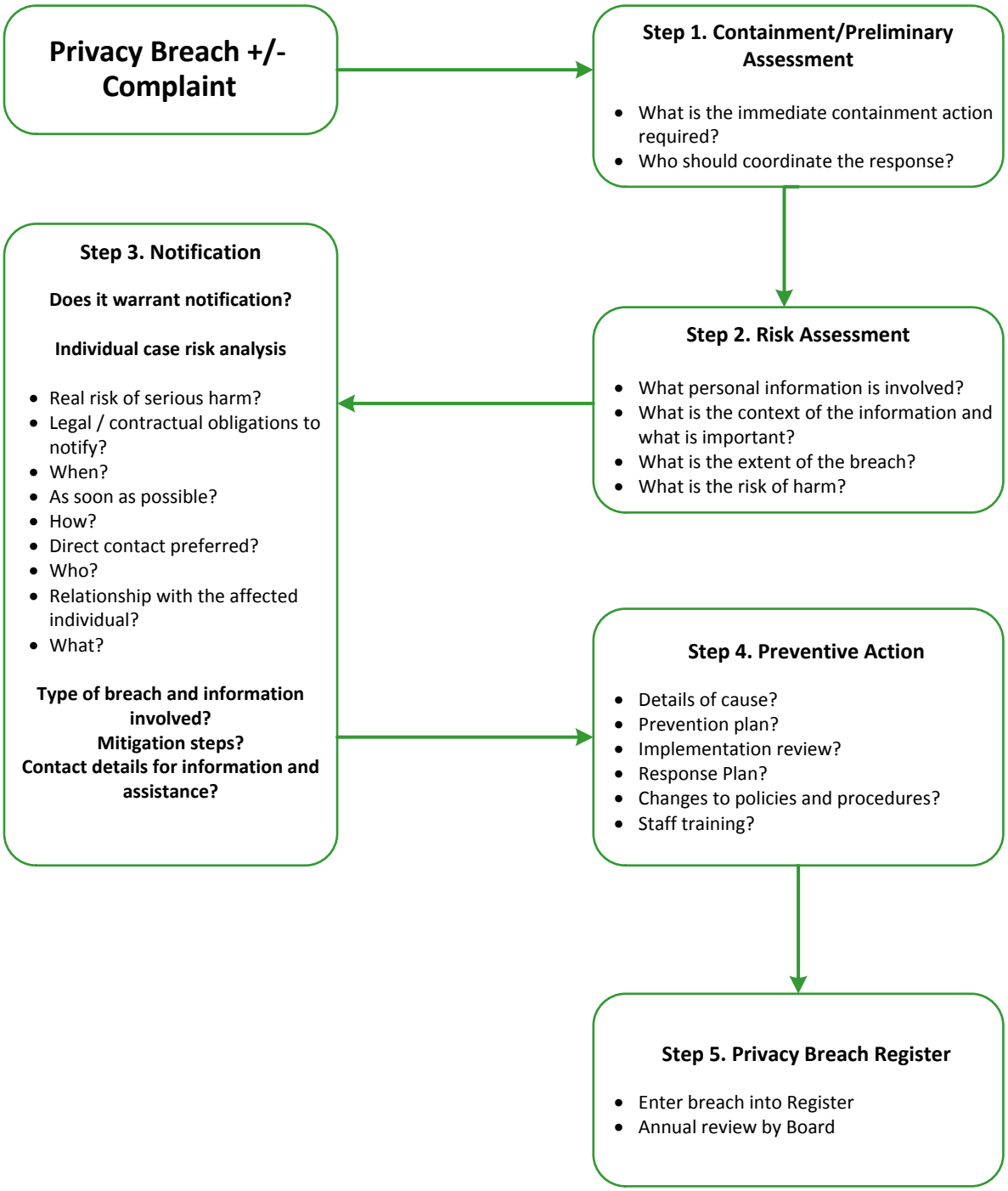
Sign off by: Chair of the Board

Signature: Ron O'Brien

Related Documents, References and Resources

- HLNT Privacy Policy
- HLNT Privacy Operational Guidelines
- NDSS Privacy Policy
- NDSS Privacy Breach Complaints Policy and Procedure
- HLNT Service Agreements with external funders
- Privacy Act 1988
- Australian Privacy Principles
- My Health Records Act
- Office of the Australian Information Commissioner, *Data breach notification guide: A guide to handling personal information security breaches*, August 2014.
- ***Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)***

Privacy Breach+/- Complaint Process Map



Employee and Contractor Privacy Policy

Policy Statement

Healthy Living NT collects personal information in order to conduct its business and comply with a range of legislative requirements and funder requirements. Healthy Living NT (HLNT) is committed to meeting our privacy obligations to you, including those set out under the *Privacy Act* 1988 (Cth) and the *Fair Work Act* 2009 (Cth).

Scope

This policy explains how HLNT handles the personal information of people who work for us and with us (such as employees, contractors, and people who work for our suppliers).

A separate Privacy policy relating to how we may collect, use, and disclose personal information about our clients and the general public, can be found here

This policy may be varied at any time.

Who and when

This policy applies to all HLNT employees, all HLNT suppliers, contractors and subcontractors, work experience students, and all HLNT volunteers (Workers).

Collection of Personal Information

1.1 How we collect personal information

(a) when you provide it to us

For example, if you apply for or commence work at HLNT, you will provide information to us as part of your application or induction. This may also include information that we are required to obtain and hold as a prerequisite of your employment, including but not limited to:

- professional qualifications, licenses, police clearances and other approvals or documentation that may be required by law or funding agreements that are reasonably required for HLNT business functions;
- information that the *Fair Work Act* 2009 requires all employers to keep certain personal information about employees in their employee records information and to keep this information secure. This may include:
  - the employee's personal and emergency contact details
  - information about terms and conditions of employment
  - wage or salary details
  - leave balances
  - records of work hours
  - records of engagement, resignation or termination of employment
  - information about training, performance and conduct
  - taxation, banking or superannuation details
  - professional, trade association or union membership information

If you work for a company that is a contractor to us, then your employer may provide us with your details.

Policy

Life. Be in it.™

(b) when someone else provides it to us on your behalf

Someone else (such as a recruitment agent or referee) may have provided us with information about you when we were assessing your suitability for work at HLNT. A colleague may provide information about you for the purpose of appraising your performance or conducting an internal investigation.

(c) when we collect it in relation to your work

We may also collect information about you and your work during the course of your employment or performance of a contract, such as information about your ingress and egress of HLNT property, your use of HLNT equipment (including computers and databases), and information collected from monitoring your use of email, to ensure you comply with our applicable policies.

1.2 Purposes for which we collect, use, and disclose personal information

The purposes for which we collect, use, and disclose personal information include:

- to establish, maintain and manage our relationship with you, including functions such as recruitment, payroll, appraisals, and any disciplinary action (including any termination of any employment or engagement) and managing your work and any claim in relation to any injuries, illnesses you have and any workers compensation claims by you;
- to assess or respond to claims, complaints, or conduct, or co-operate with investigations when required;
- to obtain professional services as required including legal, human resources, industrial relations, accounting and insurance services;
- to comply with provisions of funding agreements which specify standards regarding employees;
- for purposes directly related to all of the above;
- otherwise as permitted or required by law including to certain government agencies (such as the Australian Tax Office and Centrelink); or
- otherwise with your consent.

1.3 Disclosure of personal information

We may also disclose your personal information to enable HLNT business functions including our:

- technology service providers, including, internet service providers, cloud hosting service providers, software suppliers, maintenance and support service providers, and security services on a confidential basis so that they can provide services to us;
- external consultants such as legal, human resources, industrial relations, accounting, and insurance;
- funders, where the information is being provided to meet a lawful request; and
- travel agents and suppliers of accommodation and travel services.

Contracted third parties to whom we disclose your information, such as IT service providers, sign a confidentiality agreement that requires them to comply with the Privacy Act and our Privacy Policy.

1.4 Storage of personal information

We take appropriate steps to protect your personal and sensitive information held by us from misuse, interference, unauthorised access, modification, loss or disclosure. This includes during storage, collection, processing, transfer and destruction of the information. We are obliged to inform you should any privacy breach of your information occur.

Information is stored in secure, alarmed, access-controlled premises, within which:

- Paper files are stored in locked cabinets or rooms, and
- Electronic databases are password secured with access restricted to those staff involved in providing the services to you, within servers protected by firewalls and intrusion detection.

We take steps to ensure the security of the Healthy Living NT website. However, users are advised that there is always some risk when transmitting information across the internet, including a risk that information sent to or from a website may be intercepted, corrupted or modified by third parties.

The Healthy Living NT website contains links to external websites. We recommend that you review the privacy policies of those external websites as we are not responsible for their privacy practices.

When we no longer need, or are no longer required to keep, personal or sensitive information for any purpose we will take reasonable steps to destroy the information using confidential destruction services or ensure that the information is de-identified. This will apply except where the information is part of a Commonwealth record, or we are required by law or a court/tribunal order to retain the information.

Seeking access to, and updating, information we hold about you

You have the right to request access to your personal information that is held by HLNT about you and to request that a correction be made to the record if the information recorded about you is inaccurate.

HLNT will take reasonable steps to make appropriate corrections to personal information so that it is accurate, complete and up-to-date. To seek access to, or correction of, your personal information please contact the Finance and Administration Manager or CEO.

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

Approval

Submission Date:	Board Meeting 6/21 of 11 December 2021
Approval Date:	Board Meeting 6/21 of 11 December 2021
Circulation:	All HLNT Board Members and staff.
Sign off by:	Chair of the Board

Signature: Ron O'Brien

Related documents

This policy should be read in conjunction with the following related documents:

HLNT Privacy Policy

Privacy Breach Policy and Procedure

healthylivingNT

Data Governance Policy

1. Purpose

Knowledge and information are Healthy Living NT's most valuable organisational assets, enabling:

- effective and best practice service provision to clients and consumers
- evidence and outcomes-based planning and service delivery
- accountable and accurate reporting to funders and
- effective communications for community benefit.

This Data Governance Policy has been developed to support Healthy Living NT (HLNT) in the responsible and ethical management of its data and information assets.

Data management, as referred to in this policy, encompasses the planning, execution and oversight of policies and processes that acquire, store, protect and deliver data and information assets.

This policy contains key information for all HLNT staff and in particular those responsible for making data and associated systems-related decisions. Further, it provides guidance to key stakeholder organisations and users that provide data to, or receive data from, HLNT.

This policy forms the basis for HLNT's data governance framework and recognises that a combination of supporting policies, procedures and guides is required to achieve effective data governance and compliance with applicable legislation.

2. Scope

This policy outlines the activities required to secure, manage and distribute data held by HLNT or within HLNT's custody or control, including primary health care data, and any data stored and transmitted regardless of storage location, format or medium.

This policy applies to all employees, including duly authorised contractors.

3. Definitions

Data	can be any form of information of value to a business. It can be used as a basis for reasoning, discussion or calculation. For the purpose of this document, data refers to any information or records associated with the functioning and operations of HLNT. Data may be stored in structured (e.g. databases) or unstructured (e.g. documents) formats
Data governance	designates the source of authority for making decisions about data; the roles/structures authorised to make decisions; and the basis upon which decisions are made

Life. Be in it.™

Policy

De-identified information	is information that is not (or is no longer) about an identified or reasonably identifiable individual and does not reveal personal information about such an individual.
Personal information	is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.
Re-identification	is the discovery of the identity of individual(s) in an apparently de-identified dataset
Sensitive information	is a defined category of personal information under the Privacy Act, which includes information or an opinion about a person's racial or ethnic origin, political opinion, religious or philosophical beliefs, sexual orientation, criminal record and health, genetic and/or biometric information

4. Principles

All data containing personal information shall be collected, used, shared and managed in accordance with:

- the Australian Privacy Principles under the *Privacy Act 1988*
- the *Privacy Amendment (Private Sector) Act 2000*
- the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 and*
- the *Privacy Amendment Notifiable Data Breaches (NDB) Act 2017.*

In addition, HLNT abides by a defined set of principles which are derived from the National Aboriginal and Torres Strait Islander Health Data Principles which are considered to represent best practice in the use of information relating to the health of all Australians.

- *Data security is integral to the collection, storage, analysis and management of data at HLNT*
- *The management of health and health-related data must be ethical, transparent meaningful and useful.*
- *Data about the health of people and the services they received must be used to support improved health outcomes for people and better planning and delivery of health services.*
- *The analysis, interpretation and reporting of health and health-related data should occur collaboratively between the parties.*
- *The privacy and confidentiality of people and health service providers must be protected in accordance with the relevant legislation, standards or guidelines.*
- *Health service providers must inform people about how and why their health data is collected and used (informed consent).*
- *Data sharing is encouraged where it will assist in the planning, management and delivery of health services.*
- *Data collections require regular review and refinement by parties to monitor data quality, identify opportunities for improvement and ensure relevance to service delivery and compliance with agreed data needs.*

5. Policy Statements

5.1 Data Governance Steering Committee

HLNT will have a Data Governance Steering Committee which is responsible for directing the effective and efficient management of data/information assets in line with organisational priorities. This Committee will act as Data Sponsor, Data Custodian and Data Steward will be appointed for each data set which HLNT creates, acquires, uses or interfaces with.

5.2 Data Classification

Each data set will be classified according to its level of sensitivity, and the controls applicable to that classification will be applied.

- **Unrestricted:** Data approved as suitable for public dissemination or deemed public by legislation or routine disclosure. These data do not require additional protection and release would have no adverse impact on HLNT, other organisations or individuals. Data is de-identified, usually aggregated, and there is no risk of re-identification. Examples might include data downloaded from public web sites, public reports or other HLNT public documents.
- **Restricted:** Data that is generally available to eligible employees and designated appointees of HLNT for the purpose of carrying out HLNT business. There is some risk of re-identification. Access restrictions must be applied. Disclosure could cause low to medium impact to HLNT, other organisations or individuals. Examples might include HLNT financial information.
- **Highly Restricted**: Data which may not be accessed without specific authorisation, due to legal, ethical or other constraints. Disclosure could result in invasion of privacy by the release of personal, identifiable data, and could have a significant impact on individuals, other organisations and HLNT. All personal information, including sensitive information as contemplated in the Privacy Act, should be classified as Highly Restricted.

5.3 Data Security

HLNT will protect each dataset with an appropriate level of security in line with the data classification. Controls may include (but are not limited to): access control, password protection and encryption.

HLNT controls access to HLNT computer systems and corporate information by having a process of assigning access or permissions to corporate directories and information as appropriate based on position of the particular user in the organisation.

Permissions are assigned to individuals that are authorised to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. Individual multi-factor authentication identification is also required to access HLNT's systems.

Access to databases and other applications and levels of access are position-specific and require additional unique individual passwords which comply with the password composition requirements. Additional multi-factor authentication is required in some circumstances. Audit ability is built into database software and monitored for ongoing data security and tracing.

Contractor Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function and often in conjunction with System/Security Administrator. Access to HLNT information and systems must be approved by CEO following completion of Non-Disclosure Agreement.

5.4 Data Breach Response

Actual or suspected data breaches involving Restricted or Highly Restricted data shall, without delay, be contained, assessed and responded to in accordance with the HLNT Privacy Breach Policy and Procedure.

5.5 Privacy Impact Assessment

HLNT will conduct a privacy impact assessment for each data set involving personal information that it creates, acquires, uses or interfaces with in accordance with the OAIC Privacy Impact Assessment Guide and accompanying tool.

5.6 Data Registry

HLNT will maintain a current data registry of all data sets under its control or to which it has access. Restricted and Highly Restricted data sets. New data sets must be added as soon as acquired. The Data Registry (appendix A) will include a set of data metrics including dataset name, classification, information type, governing legislation, approved primary and secondary uses, storage type and location, access levels and retention requirements.

5.7 Data Sharing and Data Release

HLNT does not normally allow external access to any HLNT data set which is classified as Restricted or Highly Restricted. Data sharing and data release arrangements must receive the explicit approval of the HLNT Board (including formal agreements to govern the confidentiality and sharing of data). The HLNT Data Registry must note any data sets being shared.

6. Roles and Responsibilities

Data governance is the initiative HLNT takes to create and enforce a set of rules and policies regarding its data. This covers issues such as assigning accountability to teams and roles responsible for data assets and overseeing the granting or restricting access to data as required.

Typical data governance roles are shown below.

- **Data Governance Steering Committee** – responsible for directing the effective and efficient management of HLNT data assets in alignment with organisational priorities and operational needs. The DGSC is responsible for ensuring the appropriate security measures are developed, endorsed, instituted and monitored.
- **Data Sponsor** – senior level executives with control over strategic direction, who undertake duties of ownership of particular data sources on behalf of HLNT. This may be an Executive Manager or someone who reports to the CEO.
- **Data Custodian** – responsible for the day to day management and oversight of a Data Set, approval of access to data and the overall quality and security of a Data Set.
- **Data Steward** – responsible for the day to day management and operation of a Data Set, its completeness and quality.

However, in a small organisation such as HLNT these roles are jointly shared by the Executive management team and the Information Officer.

6.1 Executive Management Team and Information Officer

- The Executive Management team (comprising the CEO, Manager Education Services and Manager Finance and Administration) and the Information Officer will form HLNT's Data Governance Committee.
- Ensure all staff, including new HLNT employees, are inducted into the HLNT Data Governance principles outlined in this policy, including data-specific roles and responsibilities
- Assume Data Sponsor, Custodian and Steward roles for relevant data sets
- Lead the Data Breach Response team in the event of an incident
- Lead in the integration of Data Governance training into standard HLNT on-boarding procedures for new staff, and into the ongoing cycle of training for current staff
- Support the embedding of data-specific roles and responsibilities into relevant position descriptions

6.2 All HLNT Staff and Authorised Users of HLNT systems

- Maintain the safe and secure management of data assets within HLNT by adhering to the principles and protocols outlined in this policy and associated policies and procedures
- Complete all required training in Data Governance and Information Security

7. Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

8. Approval

Submission Date:	Board Meeting 3/22 of 18 June 2022
Approval Date:	Board Meeting 3/22 of 18 June 2022
Circulation:	All HLNT Board Members and staff.
Sign off by:	Chair of the Board
Signature:	

9. Supporting Policies, Procedures and Documents

HLNT Ethical Practice Guide

HLNT Values

HLNT Privacy Policy

HLNT Employee and Contractor Privacy Policy

HLNT Privacy Breach Policy and Procedure

HLNT Cybersecurity Policy

HLNT Clinical Governance Policy

HLNT Research Participation Policy

OAIC Privacy Impact Assessment Guide

HLNT Governing Policies:

All Personal and Sensitive Data: Access and use is governed by HLNT's *Privacy Policy* and related policies, which are compliant with the Privacy Act et.al.
Business, Governance and Financial Data: For detailed protocols, refer to HLNT's *Release of Information Policy* and *Compliance Authority Investigations Policy.*
Digital Data: For detailed information on management and security measures, refer to HLNT *Cybersecurity Policy.*
Hard Copy Data: For detailed information on management and security measures, refer to HLNT *Privacy Policy* and *Occupational and Office Health Policy* .

Data	Classification	Type	Governing Legislation	Approved Primary Uses	Permitted Secondary Uses	Storage	Access	Retention	Data Sharing
A. Information/data under the direct control of HLNT									
1. Client	**Highly Restricted**	**Personal and Sensitive data**	Privacy Act; Notifiable Data Breaches (NDB) scheme	> Provision of diabetes or cardiac and nutrition education, information and services; > Report back to health professionals; > Use of non-identifiable statistics in reports to funders and program evaluation;	> Maintenance of contact and personal detail updates in HLNT Member and NDSS DB; > Mandatory reporting; > Release of data to third parties if required to do so by law; > Release of data to third parties in an emergency situation; > Complaint management; > Health Complaints Commission; > Assessment/Notification of Data Breaches; > Legal defence proceedings; > Insurance and proceedings.	Hard copy and Digital Onsite HLNT Server	> Client: Individual personal record; > All staff: Personal Data / Diary / DB admin; > Health Professional staff: Clinical data including mandatory reporting; > Management Staff: Permitted secondary uses.	Permanent; Hard copy files may be destroyed (using confidential destruction) if record has been digitised.	No
2. Staff	**Highly Restricted**	**Personal and Sensitive data**	Privacy Act; Notifiable Data Breaches (NDB) scheme	> Employment with HLNT; > Statutory reporting to ATO and related authorities; > Compliance reporting to funding bodies; > Compliance reporting to Health and Safety authorities; > Financial Audit; > Workers Compensation Insurance	> Mandatory reporting; > Release of data to third parties if required to do so by law; > Release of data to third parties in an emergency situation; > Complaint management; > Fair Work Commission; > Assessment/Notification of Data Breaches; > Legal defence proceedings; > HLNT external advisors; > Insurance and proceedings.	Hard copy and Digital Onsite HLNT Server and HR Portal	> Staff: Individual employee record > Management and authorised Admin Staff: Approved primary and permitted secondary uses > Auditor: All uses related to financial audit	Permanent; Hard copy files may be destroyed (using confidential destruction) if record has been digitised.	No
3. Member	**Highly Restricted**	**Personal and Sensitive data**	Privacy Act; Association Act; Notifiable Data Breaches (NDB) scheme;	> Provision of education and information services; > Provision of member benefits; > Communications about HLNT; > Access to information as prescribed in the Constitution; > Use of non-identifiable statistics in reports and program evaluation;	> Maintenance of contact and personal detail updates in HLNT Client and NDSS DB; > Mandatory reporting; > Release of data to third parties if required to do so by law (subject to Constitution/Board caveats); > Release of data to third parties in an emergency situation; > Complaint management; > Assessment/Notification of Data Breaches; > Legal defence proceedings; > HLNT external advisors; > Insurance and proceedings.	Hard copy and Digital	> Member: Individual personal record; > Admin staff: Personal Data / Finance data / DB admin; > Management Staff: Permitted secondary uses > Board: Membership Approval and Dispute Resolution	Hard copy: 3 years (using confidential destruction) Electronic: Permanent	No
4. Participant	**Highly Restricted**	**Personal data** Note: some sensitive data may be collected for specific programs: management as per client data.	Privacy Act; Notifiable Data Breaches (NDB) scheme	> Provision of health promotion information, activities and programs; > Communications about HLNT programs; > Use of non-identifiable statistics in reports and program evaluation; > Identifiable participant information and statistics to funders for specific funded programs where prior consent is obtained.	> Mandatory reporting; > Release of data to third parties if required to do so by law or funding agreement; > Release of data to third parties in an emergency situation; > Complaint management; > Assessment/Notification of Data Breaches; > Legal defence proceedings; > HLNT external advisors; > Insurance and proceedings.	Hard Copy and Digital Onsite HLNT Server	> Participant: Individual personal record; > Health Promotion staff: Personal Data; > Admin staff: Personal Data / Diary / DB admin; > Management Staff: Approved primary and Permitted secondary uses.	Hard copy: 2 years (using confidential destruction) Electronic: Permanent	No

Data	Classification	Type	Governing Legislation	Approved Primary Uses	Permitted Secondary Uses	Storage	Access	Retention	Data Sharing
5. Financial	**Restricted**	**Confidential data**	Association Act ACNC Act ICAC Act Various – refer Legislation Register	All purposes necessary for the financial management of HLNT including but not limited to: > compliance reporting to the ATO and similar > financial audit > financial reports > funding acquittals > customer information > payroll > banking	> Release of data to third parties if required to do so by law or funding agreement; > Complaint/investigation management; > Legal defence proceedings; > HLNT external advisors; > Insurance and proceedings.	Hard copy and Digital Onsite HLNT Server	> Admin staff: Customer sales and transactions, purchase orders, recording of income > Finance and Management staff: All Approved and Permitted Uses; > Board: All Approved and Permitted Uses; > Banking Access: as per Delegations; > Auditor: All uses related to financial audit	Hard Copy: 7 years, unless otherwise specified (using confidential destruction) Electronic: Permanent	No
6. Board	**Restricted**	**Confidential data**	Association Act ACNC Act ICAC Act Various – refer Legislation Register	All purposes necessary for the good governance of the Association	> Release of data to third parties if required to do so by law or funding agreement; > Complaint/investigation management; > Legal defence proceedings; > HLNT external advisors; > Insurance and proceedings; > Auditor: All uses related to financial audit	Hard copy and Digital Onsite HLNT Server and Web Portal	Board and Management Staff: > All Approved uses. > All Permitted once approved by Board; > Auditor: All uses related to financial audit. Information Officer: Web portal	General Board Records: > Hard copy 7 years, (using confidential destruction); > Electronic: Permanent. Board Minutes: Permanent	No
7. HLNT Business	**Restricted**	**Sensitive**	Association Act ACNC Act ICAC Act	All purposes necessary for the conduct of HLNT corporate business, particularly: > agreements, contracts and arrangements with external funders > business and services agreements and contracts	> Release of data to third parties if required to do so by law or funding agreement; > Complaint/investigation management; > Legal defence proceedings; > HLNT external advisors; > Insurance proceedings.	Hard copy and Digital Onsite HLNT Server and Web Portal	> Board and Management Staff: All Approved and Permitted uses; > Nominated Admin Staff: Relevant uses approved by management; > Auditor: All uses related to financial audit	> Hard copy 7 years, (using confidential destruction); > Electronic: Permanent	No
B. Information/data that HLNT staff have access to									
1. NDSS Registrants	**Highly Restricted**	**Personal and Sensitive data**	Privacy Act; Notifiable Data Breaches (NDB) scheme	> Provision of NDSS services as specified in *NDSS Data Access and Usage Policy;* > Use of non-identifiable statistics in reports to funders and program evaluation;	> Maintenance of contact and personal detail updates in HLNT Client and Member DB; > Release of data to third parties (if required to do so by law/emergency situation) only if approved by DAL;	Hard copy and Digital External Database	As determined by DAL / DoH	Nil retention or extract unless explicitly approved	N/A
2. Clients at external clinics	**Highly Restricted**	**Personal and Sensitive data**	Privacy Act; Notifiable Data Breaches (NDB) scheme	> Provision of specified clinical services as determined by external clinic or funder; > Reporting to clinic/funder and specialist medical services as required; > Use of non-identifiable statistics in reports to funders and program evaluation;	> Mandatory reporting as required by law with reference to agreed framework with external clinic or funder; > Complaint management; > Health Complaints Commission; > Legal defence proceedings; > Insurance and proceedings.	Hard copy and Digital External Database	As determined by external clinic/health service	Nil retention or extract except for Approved Primary Purpose	N/A
3. External Health databases	**Highly Restricted**	**Personal and Sensitive data**	Privacy Act; Notifiable Data Breaches (NDB) scheme	> Provision of clinical services to specific clients	Nil	Hard copy and Digital External Database	Health professional staff approved by external system administrator	Nil	N/A

healthylivingNT

Cybersecurity Policy and Procedures

Policy Statement

Healthy Living NT (HLNT) is committed to maintaining integrity in its business systems and operations, health and personal data security and protecting client, member and customer privacy and confidentiality in accordance with HLNT's *Privacy Policy*.

In support of this commitment, it is HLNT's policy that information, in all its forms, written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorised modification, or destruction throughout its life cycle.

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. In a computing context, the term security implies cybersecurity.

This Cybersecurity Policy is a formal set of rules by which all people who are given access to HLNT technology and information assets must abide. The Cyber Security Policy serves several purposes:

- To describe the technology and information assets that must be protected and identify many of the threats to those assets.
- To establish standards and controls and specified levels of performance required to optimise safeguards for the system and its data.
- To inform HLNT users: employees, contractors and other authorised users of their obligatory requirements for protecting the technology and information assets of the HLNT.

This document also contains procedures for responding to incidents that threaten the security of HLNT computer systems and network and provides general practical advice to users in minimising risk.

Responsibilities

This policy sets out guidelines for generating, implementing and maintaining practices that protect the HLNT's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

	Responsibility
Board	Providing the overarching strategic view for the organisation including ensuring strong cybersecurity and corporate governance. Monitoring compliance and progress toward achievement of strategic plan. Identifying and managing risk.

Policy

Life. Be in it.™

CEO	It is the responsibility of the CEO to ensure that: • staff are aware of this policy • any breaches of this policy coming to the attention of management are dealt with appropriately • HLNT systems conform to identified standards • a cybersecurity team is appointed.
Cybersecurity Team (CEO, Manager Education Services and Finance and Administration Manager, Information Services Officer)	It is the responsibility of the cybersecurity team to ensure that: • HLNT maintains a proactive approach to any changes to the organisation's cyber security requirements; • a report on the organisation's cyber security is submitted annually to the board • Cybersecurity risk is identified and managed
Staff and volunteers	It is the responsibility of all employees and volunteers to ensure that: • they familiarise themselves with cyber security policy and procedures • their usage of cyber media conforms to this policy • unsafe or sub-optimal practices are reported • potential and/or actual security incidents are reported.

HLNT ICT Environment

HLNT operates in:

- A Citrix/thin client environment with servers based in Darwin. Specific stand-alone devices include resource PCs and laptops for use by designated positions and functions.
- A Microsoft Exchange email system located in the Darwin office. External access to email via mobile devices is not available. Inbound email is filtered by Trend Micro Hosted Email Security.
- A managed facilities environment specified in a Service Level Agreement with an external service provider (ESP), currently Area9 IT Solutions, to manage the HLNT server environment. The managed service includes monitoring of backup status, anti-virus updates and Microsoft Windows updates. Microsoft security and critical updates are applied automatically. Other updates and patches are applied as required.
- Each HLNT office has an Internet router with firewall rules configured to block unauthorised connections to the internal network. These routers also provide Virtual Private Network (VPN) connectivity between each of the offices.
- HLNT controls access to HLNT computer systems and corporate information by having a process of assigning access or permissions to corporate directories and information as appropriate based on position of the particular user in the organisation.
- In a non-public, externally accessible mode. Users of the system must have a valid logon ID and password. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet.
- HLNT also offers a publicly accessible website with private access to designated areas. This is managed externally by Brainium Labs. A Web application firewall monitors, filters or blocks the HTTP traffic to and from the site.

Definitions

Administrator	Means the overall system administrator who has access to the Administrator account, currently Area 9.
CEO	Means the HLNT Executive position responsible for ensuring the security of systems and data in HLNT (including physical security).
MES	Means the Manager Education Services
FAM	Means the Finance and Admin Manager
ISO	Means the Information Services Officer
Employees/Users	Refers to all staff, consultants, contractors and volunteers and other authorised users on HLNT's ICT assets
ESP	Refers to the external company or companies retained by HLNT under a Service Level agreement to manage HLNT's server environment
Critical infrastructure	Physical and virtual assets that are vital to the operation of HLNT
Cyberattack	An offensive act against computer systems, networks, or infrastructure.
Cybercrime	Computer-facilitated crimes, though frequently can be used to refer to all forms of technology-enabled crimes.
Cyberespionage	The practice and theft of confidential information from an individual or organisation.
Cybersecurity	The discipline and practice of preventing and mitigating attacks on computer systems
Cyberthreat	A potential threat targeting computer systems and technology, typically from the internet.
Cyberwarfare	Internet-based conflict to attack computer systems to disrupt or destroy.
DoS/DDoS	Denial of Service/ Distributed Denial of Service. A common attack involving thousands of devices accessing a site simultaneously and continually to overload its ability to serve web pages.
Hacker/Hacking	While originally in reference to a programmer 'hacking at code', it's now become mainstream to represent individuals who maliciously breach ('hack into') computers and related systems.
ICT	Information and Communications Technology. Overarching term encompassing all forms of computing and telecommunications technology inclusive of hardware, software, and networks.
IoT	Internet of Things. An evolving definition of the wide-variety of internet-connected devices ranging from sensors to smartphones.
Internet security	A general term referring to the security of internet related technologies, such as web browsers, but also that of the underlying operating system or networks.
Malware	Catch-all term to refer to any type of malicious software, typically used in reference to viruses, ransomware, spyware and similar.
Phishing	Deceptive attempt, usually over email, to trick users into handing over personally identifiable or critical information (such as passwords or credit card numbers).
Ransomware	Malware used to hold an individual or organisation to ransom, typically by encrypting files or an entire hard drive and demanding payment to 'unlock' the data. Also known as Cryptoware.
Social engineering	The practice of manipulating human beings to gain access to data or computer systems.
Spear-phishing	Highly-targeted form of phishing towards an individual or business, often utilising social engineering techniques to appear to be from a trusted source.
Spyware	Covert software designed to steal data or monitor people and systems for cybercriminals, organisations, or nation states.

Scope

All users of HLNT systems must protect HLNT's technology and information assets. This information must be protected from unauthorised access, theft and destruction. The technology and information assets of the HLNT are made up of the following components:

- Computer hardware, CPU, removable media, Email, web, application servers, PC and laptop systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols.
- Application Software: used by the various groups within HLNT. This includes custom written software applications, web applications and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.
- Telephone system hardware, software and fibre network, servers and a system management software console/portal.
- Website
- Videoconferencing facilities in both Darwin and Alice Springs offices

Threats to Security

Threats to security fall into three primary areas:

Amateur Hackers and Vandals

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favourite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of the HLNT system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

Criminal Hackers and Saboteurs

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

Employees

Because of their everyday use of the system, one of the biggest security threats is employees. Damage may be caused to the system either through inadvertent actions or on purpose. Employee awareness of cybersecurity is vital for system protection.

Risk Mitigation and Control Measures

Activity/Security Control	Requirement/Rationale	Responsibility
Acceptable Use	HLNT ICT assets are provided for HLNT business only. Use is in accordance with HLNT's *Computer Internet and Email Policy* which permits peripheral personal use in certain circumstances only	All staff
Internet Use	HLNT provides internet access to all employees and contractors for the conduct of HLNT business in in accordance with HLNT's *Computer Internet and Email Policy*	All staff
User Classification:	Defines user groups and defined the access privileges and responsibilities	
• ***Users***	Access to applications and databases specifically required for job function	All staff
• ***System Administrators***	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only. Non-Disclosure Agreement a prerequisite.	CEO, MES and FAM; ISO, ESP
• ***Contractors***	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function and often in conjunction with System/Security Administrator. Knowledge of security policies. Access to HLNT information and systems must be approved by CEO following completion of Non-Disclosure Agreement.	CEO, Contractors, ESP
• ***Members***	Access is limited to applications running on public web servers. Members may access discrete information but will not be allowed to access confidential information.	All Staff
• ***General Public***	Access is limited to applications running on public web servers. The general public will not be allowed to access confidential information.	All Staff
Access Control:	Controls access to the critical information resources that require protection from unauthorised disclosure or modification. Permissions are assigned to individuals that are authorised to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password.	All Users
• ***User System and Network Access***	All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and not shared with other staff or a third party, except where required for business purposes (eg monitoring over annual leave periods). Where this occurs a new user password must be created on return to work.	All Users/ FAM/ISO ESP
• ***Multi Factor Authorisation***	All staff with access accounts in Citrix, Nordpass and Nookal will also require an individual multi-factor authentication identification to gain access to HLNT's computer system. Where MFA is available, it must be used.	All Staff
• ***Passwords***	All users must comply with the following rules regarding the creation and systematic maintenance of passwords: • Passwords should be generated using NordPass to ensure they meet company policy on length, characters and symbols. • Passwords must be complex alpha/numeric and include symbols, and be not less than twelve (12) characters. • Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal and not sent via external email. If a password must be shared it should be shared via the secure NordPass platform. • Passwords must be added to the individual's NordPass account • Reports from NordPass will be reviewed quarterly to ensure compliance with policy. Passwords are reported on based on strength, duplication and age.	All Users/ FAM/ISO ESP

Activity/Security Control	Requirement/Rationale	Responsibility
• ***Passwords***	**Password generation:** • All passwords must be generated using NordPass to ensure compliance with policy **Citrix and Microsoft account:** • Users will be provided with passwords that meet policy requirements • MFA is mandatory and enforced for all users • User accounts will be frozen after 3 failed logon attempts. **Services handling sensitive data:** • Services handling sensitive client or HLNT data (e.g. Nookal), MFA must be used if available • Admins will enforce MFA settings wherever possible **Services without MFA:** • Users must change their passwords every 6 months where practical. **Services not owned or created by and for HLNT (e.g. remote clinic accounts):** • If the user has been provided individual login access they should endeavour to change their password every 6 months unless MFA is enabled If the account provided is shared with external users, the security of the account must be managed by the owning group or company.	
• ***Database Access***	Access to databases and other applications are position-specific and require additional unique individual passwords which comply with the above password composition requirements. Database passwords must never be shared. Audit ability is built into database software and monitored for ongoing data security and tracing.	FAM/MES
• ***User System and Network Access***	Users are not allowed to access password files on any network infrastructure component.	All Staff
	Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account from the CEO. All System Administration is handled through the ESP, including third-party software updates.	
	Requests for forgotten/need for new passwords need to be directed to the FAM or ISO	
	Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems, except for the facilitation of general NDSS transactions and appointment bookings etc. Elapsed time-out for system log-out is 10 minutes, after which staff must log back onto the system. Simultaneous log-on to multiple devices is not enabled.	
	Employee Logon IDs and passwords for IT systems and databases will be deactivated immediately if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of HLNT.	FAM/ISO

Activity/Security Control	Requirement/Rationale	Responsibility
• ***System Administrator Access***	System Administrators, network administrators, and security administrators will have access to host systems, routers, hubs, and firewalls as required to fulfil the duties of their job. All system administrator passwords will be CHANGED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of HLNT. This change is implemented by ESP and requires the permission of the CEO or HLNT authorised delegate advised to ESP and amended from time to time.	CEO, MES and FAM, ISO, ESP
• ***Special Access***	Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. This access is managed by ESP requires the permission of the CEO.	ESP, CEO
Third Party Networks	HLNT does not allow any third-party networks to access HLNT systems or data. All System Administration is handled and monitored through the ESP, including third-party software updates, secured on separate servers ensuring data security. This also includes 3CX phone system delivered by Vocus and administered by the ESP through a portal.	CEO, ESP
	HLNT does input data on third party networks such as NAV, Connect, NDSS Central and the PHN portal. These connections are isolated from HLNT data and networks and secured through individual multi-factor authentication access. HLNT utilises Nookal as its Client Management System. Nookal is password- and MFA-protected to ensure client data is always secure. Nookal data is also encrypted. HLNT also uses the third-party secure GoFAX system to send and receive client information and account administration is controlled through a portal which is password protected. HR Partner also third-party software which handles HLNT human resources, it is password protected, with access controlled through multi factor identification, managed and administered within HLNT.	All staff
Connecting Devices to Network	Only authorised devices may be connected to the HLNT network(s). Authorised devices include PCs and workstations owned by HLNT that comply with the configuration guidelines. Other authorised devices include network infrastructure devices used for network management and monitoring. Wi Fi system is managed securely through an Aruba software portal with HLNT or Guest access only through passwords. Users shall not attach to the network: non-HLNT computers or devices (for example wireless access points) that are not authorised, owned and/or controlled by HLNT. Users may attach storage devices such as USB sticks only to the Resource PCs provided in Darwin and Alice Springs, provided they have first been scanned for viruses - refer *Computer Internet and Email Policy*	All Staff
Wireless Networks	All wireless networks maintained by HLNT will be secured by password protection and encrypted by WPA2 to prevent unauthorised access to the network. HLNT Wi-Fi is managed through a password-protected portal, which manages access. It includes a Guest account which does not access HLNT's Citrix network. Staff Wi-Fi access: • Wi-Fi access is disabled 22:00 – 07:00 hours Guest Wi-Fi access: • Guests must accept HLNT policy (appended) before gaining access • Wi-Fi access is disabled 22:00 – 07:00 hours	CEO, MES and FAM, ISO ESP

Activity/Security Control	Requirement/Rationale	Responsibility
Remote Access	Only authorised persons and staff may remotely access HLNT's network. Remote access is provided to those employees and contractors that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorised connection can be remote PC to the network or a remote network to HLNT's network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.	All staff / ESP
Portable Devices	Portable devices such as laptops, iPads, mobile phones etc that can access HLNT data must be password protected	All staff
Decommissioned Equipment	All decommissioned equipment must have hard drives securely wipes or destroyed and all other identifications deleted	ISO/ESP
Unauthorised software	Users may not install personal software on HLNT ICT resources. This poses a threat to the security of the entire network. Software installation can only be conducted by ESP.	All staff
Latest security patches	The latest security patches are applied regularly in a timely manner to custom software running on the HLNT computer systems and are monitored and maintained by the ESP. The latest security patches are applied regularly to all Microsoft software running on the HLNT computer systems.	CEO, FAM, MES, ISO using ESP ESP
Latest antivirus/ antimalware	The latest antivirus / antimalware software updates are applied regularly to detect known viruses and/or malware	ESP
Unneeded services	Ensure that all unneeded services and interfaces on hosts (e.g., USB) are turned off to minimise the attack surface	ESP
Services and Applications	Ensure that the hosts only run services and applications that are absolutely necessary to minimise the attack surface	All staff
Passwords	Passwords are of sufficient complexity and are changed periodically to prevent unauthorised access	FAM
Security Audit	A security audit is managed and applied twice yearly. The audit will check / test external access, review Windows Event logs, review administrator rights and security group membership	CEO ESP ISO
File system changes	*Disable User Access* if malware is detected specifically related to crypto malware.	ESP
Security settings	All security settings on system are configured with security in mind to prevent unauthorised access	CEO MES FAM
Authentication	Authentication is required prior to gaining access to any services / applications running on HLNT computer systems, and that it cannot be bypassed to prevent unauthorised access	All staff ESP
Software updates	All software updates are properly signed and coming from a trusted source through malware protection	All staff ESP
Content Filtering	Inbound emails are scanned for malware and a broad scope of filtering is maintained through software. Process of report, isolate and quarantine is implemented by all staff.	ESP / All staff
Vendor Support	All application software and operating systems must be commercially available and/or vendor supported	CEO, FAM, MES and ESP

Activity/Security Control	Requirement/Rationale	Responsibility
Data Back-up	Routinely conducted daily, weekly and monthly and an annual back-up at 30 June. Darwin data is backed up to the Alice server and vice versa. Failure of back-up is automatically reported to ISO and ESP. ESP implements a cause investigation and informs ISO of any data loss and timelines a data restoration schedule. CEO and FAM advised of critical incidents / losses.	ESP / ISO
Data Recovery	Three options for recovering data: Windows Previous Versions, restore backups, and recover entire virtual machines.	ESP / FAM /ISO
Test Restores of backed up data	HLNT management ensure that a test restore of backed up data is performed once every six months	FAM/ESP/ISO
Scheduled cold restarts	HLNT management ensure that a scheduled cold restart of servers is performed once every six months. All UPS' must undergo a test and battery assessment annually in October.	FAM/ESP FAM/ESP
Phones	Security of phone system is checked by ESP, through a management console which is password protected.	ESP/ISO
Physical access to HLNT offices	Physical access to HLNT offices is controlled via key and access codes. Access to HLNT server locations is further controlled via additional access codes.	CEO/FAM
Staff Security Awareness	Security awareness and training for all staff e.g. identifying suspect emails, not clicking on links. The process of report, isolate and quarantine is implemented by all staff, routinely reinforced with security warnings from cybersecurity agencies and ESP.	CEO/ FAM/ MES / ISO /All staff
Website	A Web application firewall monitors, filters or blocks the HTTP traffic to and from the site. Account applications auto issue through portal to ISO who completes verification for access to website to maintain security and prevent robot intrusion. Website has security layer – https to avoid external attack – SSL certificate. Secure payment gateways in place; no credit card data stored. Maintenance Agreement in place including updates and regular, scheduled website back up.	CEO/website provider/ ISO
Zoom Rooms	Microsoft Office installations on Zoom Room computers have installed security software which is updated as required. This system is external to the HLNT Citrix computer system.	FAM/ISO ESP
Policy Effectiveness and Reporting	HLNT will collect and analyse statistical reports and data from a variety of sources to ensure compliance and evaluate the effectiveness of applications and policies. An annual report will be presented to the board detailing these findings. The data collected will include email filtering statistics, reports from ESP, password health data from NordPass and other sources where appropriate.	ISO/CEO/FAM

Monitoring Use of Computer Systems

HLNT has the right and capability to monitor electronic information created and/or communicated by persons using its computer systems and networks, including e-mail messages and usage of the internet.

It is not HLNT's policy or intent to continuously monitor all computer usage by employees or other users of its computer systems and network. However, users of the systems should be aware that HLNT may monitor usage, including, but not limited to, patterns of usage of the internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the internet and other electronic communications are being used in compliance with the law and with HLNT policy.

Penalty for Security Violation

Those people who use the technology and information resources of HLNT must be aware that they can be disciplined if they violate this policy. An employee of HLNT may be subject to discipline in accordance with processes outlined in HLNT's *General Conditions of Employment*. Breaches by contractors shall be submitted to the CEO.

The CEO may refer the information relating to the violation to regulatory authorities for consideration as to whether charges should be filed.

Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens (or has the potential to threaten) the security, integrity, or availability of the information resources on any part of the HLNT network. Some examples of security incidents are:

- Illegal access of a HLNT computer system. For example, a hacker logs onto a server
- Damage to HLNT computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a website. For example, a hacker initiates a flood of packets against a web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against another computer outside of the HLNT network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to Area 9 and HLNT management immediately. DO NOT turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

Approval

Original Submission Date:	Board Meeting 6/15 of 12 December 2015
Revision 1 Approval Date:	Board Meeting 2/17 of 22 April 2017
Revision 2 Date Approved:	Board Meeting 6/19 of 14 December 2019
Revision 3 Date Approved:	Board Meeting 6/20 of 12 December 2020
Revision 4 Date Approved:	Board Meeting 6/21 of 11 December 2021

Revision 5 Date Proposed: Board Meeting 4/24 of 17 August 2024
Revision 5 Date Approved: Board Meeting 4/24 of 17 August 2024

Circulation: All HLNT Board Members and staff.

Sign off by: Chair of the Board

Signature: Ron O'Brien

Related Documents, References and Resources

- HLNT Computer Internet and Email Policy
- HLNT Data Governance Policy
- HLNT Data Retention and Destruction Policy
- HLNT Privacy Policy
- HLNT Privacy Operational Guidelines
- HLNT Privacy Breach and Complaints Policy and Procedures
- NDSS Privacy Policy
- NDSS Privacy Breach Complaints Policy and Procedure
- HLNT Service Agreements with external funders
- Privacy Act 1988
- Australian Privacy Principles
- My Health Records Act
- Office of the Australian Information Commissioner, *Data breach notification guide: A guide to handling personal information security breaches*, August 2014.
- Computer Dictionary (resource for ICT terms and acronyms)

IT Security Dos and Don’ts

DO:

Do lock your computer when not in use

Do use strong and hard to guess passwords

Do report suspicious activity

Do pay attention to web links in emails

Do pay attention to suspicious emails

Do log-off from and fully shut down your computer at close of business

DO NOT:

Do not plug in personal devices, except to resource PCs. Scan devices for viruses first.

Do not respond to suspicious emails

Do not open attachments you are not expecting

Do not share passwords

Do not install unauthorised software

Do not be tricked into giving away confidential information

Guest Wi-Fi Access Policy

Guests must log in and accept the Healthy Living NT (HLNT) Guest Wi-Fi Access Policy before gaining access to the network.

Usage Restrictions:

The guest Wi-Fi network is provided for general internet browsing and email access only. Guests are prohibited from using the network for any illegal or inappropriate activities, including but not limited to:

Accessing or distributing illegal content

Engaging in any form of cybercrime or malicious activities

Downloading or sharing copyrighted material without proper authorization

Security Measures:

Guests are required to use secure, up-to-date devices when accessing the guest Wi-Fi network.

HLNT reserves the right to monitor network traffic to ensure compliance with this policy and to maintain network security.

Liability:

HLNT is not liable for any data loss, security breaches or other damages resulting from the use of the guest Wi-Fi network.

Guests are responsible for maintaining the security of their own devices.

Compliance:

By accessing the guest Wi-Fi network, guests agree to comply with this policy and all applicable laws and regulations.

Failure to comply with this policy may result in the termination of Wi-Fi access and potential legal action.

Cyber Security Incident Response Plan

Purpose

This document describes the process that is required to ensure an organised approach to managing cyber incidents within Healthy Living NT (HLNT) and coordinating response and resolution efforts to prevent or limit damage that maybe caused.

Context

Cyber security relates to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat.

It is commonly recognised that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through the alignment of people, processes and tools.

Policy

Healthy Living NT
Ph: 08 8927 8488 F: 08 8927 8515
E: info@healthylivingnt.org.au
www.healthylivingnt.org.au

Contents

1. Terminology and definitions

1.1. What is a cyber event?

A cyber event has the potential to become, but is not confirmed to be, a cyber incident. Examples of cyber events include (but are not limited):

- Multiple failed sequential logons for a user
- A user has disabled the antivirus on their computer
- A user has deleted or modified system files
- A user restarted a server
- Unauthorised access to a server or system.

1.2. What is a cyber incident?

A cyber incident occurs when there is a breach of explicit or implied digital security policy that requires corrective action because it threatens the confidentiality, availability and integrity of an information system or the information the system processes, stores or transmits.

Examples of cyber incidents include (but are not limited to):

- Denial of service attacks (DoS) that affect system or service availability
- Virus or malware outbreak (including ransomware)
- Compromise or disclosure of sensitive or personal information
- Compromise of network credentials or an email account.

This plan identifies four categories of cyber incidents which are differentiated by the level of impact they create.

2. Roles and responsibilities

2.1. Cyber Security Incident Team (CSIT)

Who	Role in CSIT
Information and Services Officer	Coordinate Assess and collect information Report to Area 9 Liaison with and reporting from Area 9 Communicate to staff Preliminary notification to Insurer
Finance and Administration Manager	
Chief Executive Officer	Coordinate Communicate with Board / Executive Board Communicate to external stakeholders (where indicated)

2.2. HLNT Board

Who	Responsibility
Board	Providing the overarching strategic view for the organisation including ensuring strong cybersecurity and corporate governance. Monitoring compliance and progress toward achievement of strategic plan. Identifying and managing risk.

Healthy Living NT
Ph: 08 8927 8488 F: 08 8927 8515
E: info@healthylivingnt.org.au
www.healthylivingnt.org.au

Who	Responsibility
Executive Board	Is responsible for the day-to-day operations of the Association between Board Meetings Carries the authority to maintain the 'business' of the Association within Board determined limits Is responsible for reviewing and reporting to the Board on any developments, which significantly impact on the organisation or its operations and for monitoring strategic directions.

2.3. HLNT Crisis Communication Team (CCT)

More serious cyber incidents may require the CCT be formed. The Crisis Communications Team may be formed by the Executive Board or Board. CSIT members are automatic members of the CCT

The response group would provide strategic oversight and make decisions/recommendations on external communications and the general operation of HLNT

See document *Crisis Communications Strategy*

3. Incident Response Process

Quick reference list of incident response actions:

#	Activity
1	**Detection:** Suspected event and or incident to be reported in CSIT
2	**Collect information:** CSIT to Identify affected staff and collect information. *This only applies if internal staff identify a suspected vent or incident*
3	**Report:** CSIT to report suspected event or incident to external IT provider (Area 9) via phone
4	**Management and Communication:** Internal and external (if necessary)
5	**Stand down:** Incident/event resolved

3.1. Step 1: Detection

There is no single process for detecting a cyber incident. Detection often involves:

- **Precursors:** detecting that a cyber-attack might occur in the future, such as the receipt of a threatening email or news of a global malware/ransomware attack (note: this form of detection is rare).
- **Indicators:** detection that an incident may have occurred (e.g. intrusion detection alerts, file names with odd characters, configuration changes).
- **Security Monitoring:** Referral from a managed security service provider or another organisation/stakeholder, alerting to the presence of a cyber incident.

Indicators	Examples
Reports of unusual or suspicious activity by staff or external stakeholders.	A staff member receives an email asking them to confirm their network credentials or to provide other personal or sensitive information.
	Multiple staff report being 'locked out' of their network accounts.
	An external stakeholder reports receiving spam or phishing emails from your organisation.
	A member of the public approaches your organisation to report the discovery (or exploitation) of a security vulnerability.
System(s)/service(s) not operating or functioning as expected	For example, one or more IT systems or services may cease functioning, or may not function as expected, and there is not a readily identifiable cause (such as a planned upgrade or outage).
	SSL Certificates broken; for example customers complaining that your organisation's website has a broken link.
Unusual Activity	Network administrators observe a large number of 'bounced' emails containing suspicious or unexpected content; or there is a substantial change in network traffic flows with no readily identifiable cause.
	Network or application logs show multiple failed login attempts from unfamiliar remote systems, such as overseas locations.
	Anti-virus alerts – a notification from your anti-virus service or a managed service provider that it has detected suspicious activity or files on your network, which require analysis and remediation.
	Service or admin accounts modifying permissions; admin accounts adding standard users to groups; service accounts logging into a workstation.
	A system administrator observes a filename with unusual characters, or expected files are no longer visible on the network.

3.2. Step 2: Collect information

If a Cyber event or incident has been reported by HLNT staff the CSIT should gather as much information as possible from affected staff. It is important that they check if additional staff members or services are affected. This information is to be passed on to the external IT provider (Area 9)

The CSIT should note:

- **What:** Ask reporting staff member/s what they were doing before they identified the potential incident
- **When:** Note the time of day it occurred as accurately as reporting staff can recall
- **Who:** note which staff are affected – including their username (what they use to log in)
- It is not recommended that HLNT take any action at this stage, but if anything was done by HLNT staff in response to a suspected cyber incident it should be noted and reported back to Area 9.

3.3. Step 3: Report

As soon as practical the CSIT must report suspected cyber incidents to Area 9 for investigation and resolution. It is important that the CSIT provides as much information as possible.

A support ticket must be lodged via a phone call to the Area 9 helpdesk:

1. **Serious Incident identified:** If the CSIT has identified a serious incident they must advise the Area 9 helpdesk by phone and inform them of the high severity nature of the incident. Additionally, CSIT should contact at least one of the contacts listed below:
    - **a.** Johnny Politis, Director Service Delivery
    - **b.** Ben Cavanagh, Service Delivery Manager
    - **c.** Brandon, Team Leader Service Delivery

    A decision as to whether to form a Crisis Communication Team may also need to be made depending on severity

2. **Suspected incident:** Report to the Area 9 help desk. Area 9 will investigate and assign a priority level (Low, Medium, High or Critical). This priority level may change as Area 9 investigates.

Reference document ***Area9's Cyber Security Response and Controls***

Area 9 has a ***Post Incident Report process*** which can be used for major events outlined at the end of this document. For other events or incidents that are significant but don't require insurance claims Area 9 can provide a summary of what occurred and recommendations.

3.4. Step 4: Manage, Communicate and Engage

3.4.1. Manage

Following initial assessment of the severity of the cyber incident by Area 9 and recommendations for rectification, the CSIT will assess and authorise initial remedial actions. At this point the CSIT will assign a severity classification to the incident, noting that this classification may increase or decrease over time with the results of further investigations and/or remedial actions. Classification factors could include:

- Effects of the incident (confidentiality, integrity and availability of information and systems)
- Stakeholders affected (internal and external)
- Incident type
- Impact on HLNT and community.

The following table is to be used as a guide when assigning a severity classification:

Incident Classification	Description
Critical (Priority 1)	• Over 80% of staff (or several critical staff/teams) unable to work • Critical systems offline • High risk to/definite breach of sensitive client or personal data • Financial impact greater than $100,000 • Severe reputational damage – likely to impact HLNT long term.
High (Priority 2)	• 50% of staff unable to work • Non-critical systems affected • Risk of breach of personal or sensitive data • Financial impact greater than $50,000 • Potential serious reputational damage.
Medium (Priority 3)	• 20% of staff unable to work • Small number of non-critical systems affected • Possible breach of small amounts of non-sensitive data • Financial impact greater than $25,000 • Low risk to reputation.
Low (Priority 4)	• <10% of non-critical staff affected temporarily (short term) • Minimal, if any, impact • One or two non-sensitive/non-critical machines affected • No breach of data • Negligible risk to reputation.
Informational (Priority 5)	• A security event with no impact to information asset and business continuity. Examples include: o Spam email with no embedded URL's or attachments o Automated malware detection alert requiring no further action. Single device, infection cleaned o General cyber security advice o False positive security alerts.

Cyber incidents with severity classifications of:

- Priority 4 and 5 are to be managed within normal business operations.
- Priority 1, 2 or 3 are to be:
  - communicated to the Board/Executive Board which will determine appropriate actions including whether to form a Crisis Communications Team
  - notified to HLNT's insurer.

3.4.2. Internal Communications

It may be necessary to brief employees about a cyber incident. This is important if organisational IT networks, systems or applications no longer operate as expected, or if the situation has potential to generate media or public interest.

Key messages to consider when communicating with employees include:

- What happened and why did it happen?
- What will happen in the immediate future?
- What are employees expected to do?
- Who can employees contact if they have questions?

All internal communications must be reviewed and approved by CSIT or the CCT (if formed)

3.4.3. External Communications

Depending on the impact and severity of a cyber incident, it may be necessary to communicate with external stakeholders (including ministers, stakeholders and funders, media and the public). This is particularly important if the incident affects systems or applications relied upon to run HLNT, or if client data has been compromised

Key messages to consider when communicating with external stakeholders include:

- What happened and why did it happen?
- What systems/services are affected?
- What steps are being taken to resolve the situation?
- Is it possible to say when the situation will be resolved?
- What are external stakeholders expected to do?
- Who can external stakeholders contact if they have questions/concerns?

All external communications to be handled by the CCT.

If, upon investigation, Area 9 finds that confidential, personal or sensitive data has been accessed, stolen or potentially accessed or stolen, the CCT is to oversee the development of specific communications strategies, plans and initiatives.

Where personal or sensitive data has been breached, HLNT's Privacy Breach and Complaints Policy and Procedure is to be activated.

3.5. Step 5: Stand Down

If the CCT was activated, it should now be stood down as soon as practical.

The CSIT should gather copies of all notes taken during the response effort to assist with a Post Incident Review with all staff and the CCT (if formed)

3.6. Step 6: Learn and Improve

The CSIT (and CCT, if activated) should come together for a Post Incident Review to discuss:

- Review incident report supplied by Area 9 and any recommendations provided
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organisations have been improved?

- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

The discussion should be documented and any key insights / lessons learnt shared with all parties involved. Any recommendations to arise from the discussion should be documented in a corresponding action plan that states how the recommendation will be actioned, by whom and when. The Cyber Security Response Plan should then be updated to reflect these actions to ensure preparedness for similar events in the future.

4. Relevant documents

- Area9's Cyber Security Response and Controls V2 - Healthy Living NT (attached)
- Area9's Post Incident Report Process (attached)
- Cyber Security policy
- Computer use policy
- Crisis Communications Strategy
- Privacy Breach and Complaints Policy and Procedure

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

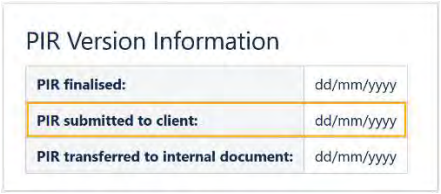
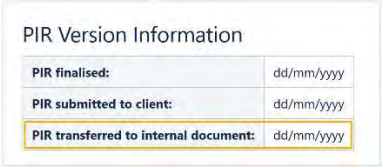
Approval

Original Submission Date: Board Meeting 3/25 of 14 June 2025
Original Approval Date: Board Meeting 3/25 of 14 June 2025
Circulation: All HLNT Board Members and staff.
Sign off by: Chair of the Board

Signature: William De Decker

Healthy Living NT
Ph: 08 8927 8488 F: 08 8927 8515
E: info@healthylivingnt.org.au
www.healthylivingnt.org.au

Area 9 Post Incident Report Process

	Name	Action	Owner	Notes
		If **a customer copy is not required;** *Step 9, Create Corrective actions*.		
8	**Export copy to PDF and provide to customer**	Utilising the **Export PDF** button at the top of the PIR, export a copy of the PIR. Review the document to confirm format and look and feel are appearing as expected. Send a copy of the PIR to the requester. Update the date within the PIR with the date the PIR has been supplied to the customer.	Business unit manager	**Export to PDF button;** If this is not available on the PIR, speak to Enterprise Support.  **PIR milestone information;** This table is excluded from the PDF export. 
9	**Create corrective actions**	Update the PIR with the date the document has been transferred to an internal document. Create a Jira ticket for each corrective action identified and link the ticket into the PIR for tracking. **Note:** *Log the ticket type as appropriate for the action or recommendation. For example; small actions would be created as Requests or Tasks within the appropriate business unit project. Larger bodies of work would be logged as Improvements or Projects.*	Business unit manager	**PIR milestone information;** 

healthylivingNT

Data Retention and Destruction Policy

1. Background

Healthy Living NT must comply with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs) and any other applicable privacy laws.

Healthy Living NT also has legal obligations to keep certain kinds of data on record for a specified amount of time. The table in Appendix 1 sets out the legally required retention periods for common categories of data.

This policy sets out Healthy Living NT's approach to managing, retaining and destroying records and data (including personal information) we hold, to ensure compliance with the APPs and data retention laws.

The purpose of this Policy is to outline roles, responsibilities and steps Healthy Living NT and staff must take when dealing with record and data retention and destruction. This policy does not cover all circumstances that may arise and is not a comprehensive statement of the relevant law. If you are unsure or have any questions about this policy, or Healthy Living NT's obligations, you should consult your manager or the CEO.

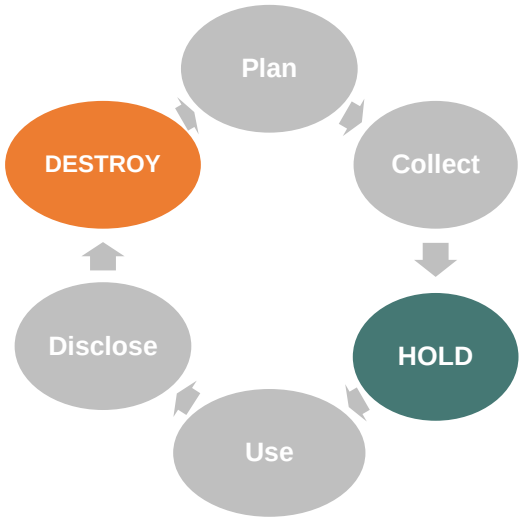
2. Scope

The Privacy Act provides that a *record* can be a paper document or an electronic file. Records may include physical documents, digital scans of documents, databases and electronic files such as text, image, video, or audio files. In essence, any medium that captures and contains information constitutes a 'record'.

In this policy, *data* means any information which is contained in a record, including (but not limited to) personal and sensitive information.

This Policy applies to all employees, including contractors and volunteers who have access to Healthy Living NT records and data or who are involved in the process of collecting, storing or securing Healthy Living NT records and data on behalf of Healthy Living NT (HLNT).

3. Information lifecycle



Policy

Life. Be in it.™

a) The information lifecycle describes each phase of HLNT records and data.

b) This policy focuses on the *Hold* and *Destroy* phases. ***Hold*** refers to how records and data are recorded, stored, secured, backed-up and archived, while ***Destroy*** refers to how records and data are disposed of or put beyond use. For personal information, *Destroy* also covers the de-identification of that information so that it is no longer considered personal or sensitive information.

c) The Privacy Act requires us to delete personal information when no longer required (which includes for any legal purpose), but data retention laws may require us to keep that personal information for certain periods of time. Privacy laws and data retention laws may appear to conflict but it is essential to consider both obligations together.

d) You must consider and apply the guiding principles set out below when managing, retaining and destroying records and data.

4. Guiding principles on managing, retaining and destroying records and data

a) Actively and continuously consider whether retention of data is necessary.

b) Do not destroy records and data that are necessary for HLNT's business functions or legally required to be kept.

c) Do not destroy records and data that may be relevant to ongoing or anticipated disputes, litigation or regulatory investigations. Consult with your direct manager or the CEO if you have doubts about whether certain records or data should be retained for their evidentiary value.

d) **Retain only minimum data necessary.** It is possible to have too much data. Over-collection of data is a significant risk. Only keep what is reasonably necessary for HLNT's business functions or to comply with our legal or clinical obligations.

e) **Consider whether** HLNT has contractual obligations to destroy certain records and data after the expiration of a contractual relationship.

f) **Record data in the most appropriate format and minimise paper records.** Scan physical documents and save the digital scans in HLNT's document management system. Do not use your email inbox as a record filing system.

g) **Take steps to secure your records and data and minimise risk of corruption of data or accidental loss**. Ensure that important data is securely backed-up and archive records when they are not actively being used (but which are not ready to be destroyed).

h) **Ensure data can be easily located and accessed** (even when archived or not in active use).

i) **Ensure paper records are securely destroyed if appropriate**. Use shredders or Confidential Destruct bins to destroy paper records.

5. Steps to Manage Data

Step 1: Identify record, data and purpose

Step 1 is to identify:

a) the data that you deal with and the records in which they are contained (i.e. certain data may be in multiple records)

b) the purpose for which the data was collected

c) the purpose for which the data (and record) is currently being held.

The data and records that you deal with in your day-to-day activities will depend on your role. For example, an employee in our finance and administration section may regularly collect and handle employee and contractor for payroll purposes and to comply with our legal obligations including:

- tax file numbers in records relating to employees
- role and salary information
- identification documents (records such as scanned passports and drivers' licences)
- contact information
- health information

An employee in providing or supporting the provision of client education services will regularly collect and handle client information including:

- Address and contact information
- Demographic information
- Health information
- Consent information

To identify the kinds of data you handle, and what possible obligations may attach to them, ask yourself:

- What data do I use to carry out my functions?
- Does that data contain personal information about individuals?

Step 2: Determine whether it is necessary to retain the data (and relevant records) and for how long.

Data is sometimes collected for one-time use, and once the purpose for which it was collected is fulfilled, it is not necessary to retain it. In such circumstances, you should promptly delete or destroy the data (and relevant records), especially if it contains personal information about individuals, to minimise the risk of that data being compromised in the event of a data breach. This is particularly important in relation to government issued identifiers such as passport and drivers' licence numbers.

Certain data (and relevant records) must be retained because they are necessary for HLNT's business functions, or because the law requires that the data be retained for a specific period of time. If you determine that it is necessary to retain the data and record identified in Step 1, determine whether it falls into a category with a specific retention period (see **Appendix 1**) so, you should take reasonable steps to ensure that the data is destroyed after that period has elapsed (see Step 4).

If the data and relevant records do not fall into a specific category, but are required to be retained, best practice is to retain the data (and relevant record):

Type	**Retention Period**
Financial and governance records	Seven (7) years
Personal information about an adult	Seven (7) years
Personal information about a child	Seven (7) years after a child turns 18
Sensitive information, including health information	Fifteen (15) years after the date of last access or forty-five (45) years after the date of birth where the client is a minor, whichever is the latest.

Consult with your manager or the CEO for advice on determining the appropriate retention period for records and data that do not fall into a category set out in **Appendix 1**.

Step 3: Decide how, and in what format, the data should be held.

If the data is recorded in hard copies (i.e. paper records), the general rule is that the document should be scanned and stored electronically and that the physical paper copy should be securely destroyed. An exception applies to original versions of documents which are legally required to be retained (see **Appendix 1**) or which HLNT may be required to produce as evidence in a dispute, legal proceedings or an investigation.

Consider whether the data (and relevant records) will need to be regularly accessed or whether they should be archived. In either case, the data (and relevant records) should be held in a manner which allows them to be easily located, accessed and retrieved when needed. If you decide to archive the data, be sure to record the date the data was created, the date it was archived, and the date after which it should be destroyed.

Data should be stored securely and in a manner that is appropriate to the value and sensitivity of the data, and the physical properties (if applicable) of the record (for example, paper records should be stored in a cool, dry place outside of direct sunlight to avoid degradation).

As a general rule, email inboxes and mailbox folders should not be the primary source of storing records and data, particularly data which consists of personal information or sensitive information. File records with personal information, sensitive information, financial information or government identification numbers in HLNT's document management system, client electronic record system or external portals such as NDSS Central as appropriate.

Step 4: Determine whether and how the data should be destroyed, put beyond use, or de-identified.

In most circumstances, data (and the relevant record) should be destroyed using Confidential Destruction (or equivalent) after its retention period has elapsed and it is no longer required for a business function or to comply with a legal requirement.

There may be occasions where it is not possible or practicable to irretrievably destroy data (because, for example, the system on which the data is stored does not allow data to be deleted or where the data is part of a larger dataset). These circumstances should be avoided if possible, but if they arise, you should take reasonable steps to

a) **put the data beyond use**. The Office of the Australian Information Commissioner (OAIC) has said this means HLNT:
   - is not able (and will not attempt) to use or disclose that data, and
   - cannot give any other entity access to that data, and
   - surrounds the data with appropriate technical, physical and organisational security. This should include at a minimum, access controls including logs and audit trails, and
   - commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible; or

b) **de-identify the data**: If the data contains personal information or sensitive information, consider whether it is possible and practicable to de-identify the data. This means taking steps to remove information that could reasonably identify an individual (for example by redacting scanned documents).

There may be certain circumstances in which the data should be de-identified immediately (such as where it is being used for analytics or research purposes, which does not require individuals to be personally identifiable.

6. Roles and Responsibilities

HLNT management is responsible for:

a) Determining retention periods for the records they hold, having regard to:
   - legally required retention periods (see Appendix 1)

- whether the retention of the record or data is (and continues to be) necessary for one or more of HLNT's functions and activities
- whether the record or data (and the relevant record) may hold evidentiary value in an existing or potential dispute, legal proceeding or regulatory investigation
- the guiding principles set out in section 4.

b) Ensuring that records and data are securely held, and that appropriate roles, responsibilities, practices and processes are put in place to ensure that records and data are destroyed after relevant retention period has ended.

c) Taking reasonable steps to destroy, de-identify or put beyond use records and data once the retention period has elapsed.

d) Seeking external advice where necessary in relation to:

- practices and procedures relating to storage and security of records, and destruction of records and data
- determining appropriate retention periods and confirming whether certain records or data should be destroyed or retained.

e) Communicating and ensuring HLNT complies with its obligations under this policy.

f) Assigning specific roles and responsibilities to team members to carry out the obligations set out in this policy.

g) Providing training on records, retention periods, and destruction practices and procedures to team members.

h) Undertaking periodic reviews of records and data held to ensure that records and data are being destroyed after their retention period has ended.

Employees, contractors and volunteers must:

a) Consider the legal obligations relating to retention and destruction of the records and data they deal with

b) Comply with obligations to:

- retain necessary and important data
- destroy unnecessary records and data
- seek guidance and direction from management where appropriate.

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

Approval

Original Submission Date: Board Meeting 2/24 of 20 April 2024
Original Approval Date: Board Meeting 2/24 of 20 April 2024

Circulation: All HLNT Board Members and staff.

Sign off by: Chair of the Board

Signature: Ron O'Brien

Supporting Policies, Procedures and Documents

HLNT Ethical Practice Guide

HLNT Values

HLNT Privacy Policy

HLNT Employee and Contractor Privacy Policy

HLNT Privacy Breach Policy and Procedure

HLNT Cybersecurity Policy

HLNT Data Governance Policy

HLNT Clinical Governance Policy

HLNT Research Participation Policy

Appendix 1: Data Retention Requirements

Document type	Examples (non-exhaustive)	Source of obligation	Retention requirement	Destruction requirement
A. Governance and financial records				
Written financial records that: • correctly record and explain HLNT's transactions, financial position and performance; and • enable true and fair financial statements to be prepared and audited.	• invoices, receipts, cheques etc • documents of 'prime entry' (receipts and payment journals) • working papers and other documents used to explain the methods by which financial statements are made up • delivery dockets • invoices and statements issued • petty cash book • bank deposit book	*ACNC Act 2012 (Cth)* *Associations Act 2003 (NT)*	Seven years after the transaction covered by the records is completed.	Destroy after retention requirement.
Books	• Books containing the minutes or proceedings of any general meeting, or meeting of the directors	*ACNC Act 2012 (Cth)* *Associations Act 2003 (NT)*	Permanently while the organisation operates. For five years after the organisation is wound up. Books must be maintained for five years from date of deregistration.	
Registers	Register of members	*ACNC Act 2012 (Cth)* *Associations Act 2003 (NT)*	Permanently	Do not destroy.
Documents relevant to income and expenditure	An organisation carrying on a business must keep records that show and explain all transactions and other acts that are relevant for ascertaining the income and expenditure.	*Income Tax Assessment Act 1936* (Cth) s 262A *Income Tax Assessment Act 1997* (Cth) s 121–25 *Taxation Determination* TD 2007/2	Five years after records prepared or obtained, or five years after the completion of the transactions or act to which the records related, whichever is later (subject to limited exceptions). CGT records must be retained for five years after it becomes certain that no CGT event can happen for which those records could reasonably be expected to be relevant to working out a capital gain or loss.	Destroy after retention requirement.

Appendix 1: Data Retention Requirements

Document type	Examples (non-exhaustive)	Source of obligation	Retention requirement	Destruction requirement
Payroll tax	Records to demonstrate and accurately calculate liability for payroll tax	*Payroll Tax Act 2009* (NT) s 74 & *Taxation Administration Act 2008* (NT) s 79	At least five years after the payment was made or obtained, or the date of completion of the transaction or act to which it relates, whichever is later.	Destroy after retention requirement.
Stamp duty and duties	Records, books, documents and working papers relating to: • transfer of property • mortgages and other security documents • leases • transfer of motor vehicles • insurance	*Stamp Duty Act 1978* (NT) & *Taxation Administration Act 2007* (NT) s79	At least five years after the date payment was made or obtained, or the date of completion of the transaction or act to which it relates, whichever is later.	Destroy after retention requirement.
Goods and services tax	Records relevant to taxable supply, taxable importation or creditable acquisitions and importations.	*Taxation Administration Act 1953* (Cth) ss 385-5	At least five years after the completion of the transaction or acts to which they relate.	Destroy after retention requirement.
Personal property security documents	Any security agreement or contract that provides for the security interest.	*Personal Property Security Act 2009* (Cth) ss 275–277	The security agreement or contract which creates the security must be retained for the term of the security. An interested person may ask a secured party who holds a security interest to send or make available to the interested person, or any other person, a copy of the security agreement that provides for the security interest, a statement setting out the amount or obligation that is secured pay the security interest and the terms of payment or performance.	Destroy after retention requirement.

Appendix 1: Data Retention Requirements

Document type	Examples (non-exhaustive)	Source of obligation	Retention requirement	Destruction requirement
Documents required as evidence in legal proceedings	The types of document that could be captured are broad. State and Territory-based legislation imposes offences in relation to the destruction of documents that a person knows are reasonably likely to be required as evidence in a legal proceeding. For example, where there has been a workplace injury or death, the reports regarding this may be required if it is criminally investigated or if the individual initiates a civil action.	Criminal Code Act 1983 (NT)	Necessary to determine on a case by case basis. Where litigation is on foot, or is reasonably anticipated, relevant documents must not be destroyed (even if this results in their retention for periods in excess of the time limits imposed by taxation, corporation or other legislation).	HLNT must take steps as are reasonable in the circumstances not to destroy documentation that could be required as part of a legal proceeding.
B. Information about individuals				
Personal information	Any document which records information or an opinion about an identified individual or an individual who is reasonably identifiable. For example, personal information may include: • name, date of birth, postal address or email address of an individual • a government issued identifier (Medicare, passport or concession card number) • feedback provided in relation to an unsuccessful applicant's job interview • professional qualifications held by an individual. Documents such as:	*Privacy Act 1988* (Cth) APP 11	Retain until the personal information is no longer required for any purpose and the organisation is not legally required to retain the information.	HLNT must take steps as are reasonable in the circumstances to destroy the personal information or to ensure that the personal information is de-identified when it is no longer needed and retention is not required.

Appendix 1: Data Retention Requirements

Document type	Examples (non-exhaustive)	Source of obligation	Retention requirement	Destruction requirement
	• job applications, reference letters • those created for, or collected through, disciplinary hearings and practice audits.			
Sensitive information, including health information	'Sensitive information' is a subset of 'personal information' and includes information about a person's: • racial or ethnic origin • religious beliefs or affiliations • sexual preferences or practices • criminal record • health • political opinions • membership of a political, professional or trade association or trade union. Documents that might contain sensitive personal information include: • records that include the criminal history of a client, contractor or job applicant, and	*Privacy Act 1988* (Cth) APP 11	Retain until the sensitive information is no longer required for any purpose for which it may be used or disclosed under the Privacy Act and the organisation is not legally required to retain the information. If the sensitive information is health information and it was collected while the person was a child, it must be retained until they reach the age of 25, or in any case seven years after the last occasion on which a health service was provided to the individual by the provider, whichever is the later. If HLNT was not the health service provider in respect of that health information, it must be destroyed or de-identified if it is no longer needed for the purpose for which it was collected.	As above, HLNT must take steps that are reasonable in the circumstances to destroy the documents containing sensitive information or to ensure that the documents containing sensitive information are de-identified when they are no longer needed and retention is not required. Where sensitive information is involved, the reasonable steps required to destroy the information under Australian Privacy Principle 11.2 by HLNT may be more onerous.
Sensitive information, including health information	• records that include medical or health information about an individual.	**NT Department of Health *Records Disposal Schedule: Patient and Medical Records***	**Fifteen (15) years after the date of last access or forty-five (45) years after the date of birth where the client is a minor, whichever is the latest.**	Destroy after retention requirement.

Appendix 1: Data Retention Requirements

Document type	Examples (non-exhaustive)	Source of obligation	Retention requirement	Destruction requirement
Government related identifiers	Tax file number	*Privacy Act 1988* (Cth) ss 17 & 18 *Privacy (Tax File Number) Rule 2015 r 11*	Reasonable steps must be taken to protect the TFN information from misuse, loss, unauthorised access, modification or disclosure. Access to such documents must be restricted to individuals who need to handle the information for taxation law, personal assistance or superannuation law purposes.	A TFN recipient must take reasonable steps to securely destroy or permanently de-identify TFN information of an individual where it is no longer: • required by law to be retained • necessary for a purpose under taxation law or superannuation law.
	Documents that fall within the concept of personal information where the identity of the individual is reasonably identifiable, including: • Medicare number • driver's licence number • passport number • Centrelink number	*Privacy Act 1988* (Cth) APP 9 & 11	See above as for Personal Information	See above as for Personal Information.
C. Employee records				
Records of employee information prescribed by Fair Work legislation	Must keep records containing prescribed information, including: • employee's name, employer's name, employee status (full-time/part-time; permanent/casual; date employment began) • records relating to pay, bonuses, allowances etc • records relating to leave • records relating to overtime	*Fair Work Act 2009* (Cth) s 535, Ch 3, Part 3-6, Division 3 *Fair Work Regulations 2009* (Cth)	Seven years after termination of employment	Destroy after retention requirement.

Appendix 1: Data Retention Requirements

Document type	Examples (non-exhaustive)	Source of obligation	Retention requirement	Destruction requirement
	• records relating to averaging of hours • records relating to superannuation contributions • records relating to termination and how employment was terminated • records relating to individual flexibility arrangements and guarantees of annual earnings.			
Records of transactions and other acts for the purpose of ascertaining an employer's liability for fringe benefits tax	Documents such as: • invoices, receipts, logbooks etc • employee declarations	*Fringe Benefits Tax Assessment Act 1986* (Cth) s 132	Five years after the completion of the transactions or acts to which the records relate.	Destroy after retention requirement.
Records which record and explain all transactions and other acts engaged in by an employer, or required to be engaged in by an employer, for the purposes of superannuation guarantee	Documents such as: • superannuation guarantee calculations; • superannuation guarantee contributions; and • choice of superannuation fund forms/nomination forms.	*Superannuation Guarantee (Administration) Act 1992* (Cth) s 79	Five years after the records were prepared or obtained, or the transactions or acts to which those records relate, whichever is later.	Destroy after retention requirement.
Record of a notifiable incident involving an employee	Records of deaths, serious injuries or illness and dangerous incidents.	*Work Health and Safety (National Uniform Legislation) Act 2011* (NT) s 38	Five years from the day notice of the incident is given to the regulator.	Destroy after retention requirement.

Artificial Intelligence Governance Framework

1. Purpose

Artificial intelligence (AI) has enormous potential to benefit community organisations. However, its use also brings risks. The Board and executive of Healthy Living NT are responsible for being aware of these risks and managing them in relation to decision-making processes and the organisation's use of AI generally.

2. Scope

The AI governance framework offers guidance to the Board and executive regarding decision making about the use of AI in Healthy Living NT.

To mitigate risks, Healthy Living NT has established guidelines for the use of AI systems, ensuring human oversight, fact-checking procedures, transparency in decision-making and ethical considerations.

3. Key Principles

Healthy Living NT's Board and staff should be aware of the limitations, risks and potential biases of AI-generated content and AI systems and must draw on human expertise and ethics to ensure transparency and accountability in decision-making and quality assurance of material produced with assistance of AI.

It is expressly forbidden to use AI systems for the automated delivery of services or recommendations to customers or clients or for screening, assessment or decision making in respect of clients or employees.

4. Policies

Policies related to the use of AI at Healthy Living NT are:

- Acceptable Use of Artificial Intelligence Tools and Models
- Ethical Practice Guide
- Consumer Charter
- Healthy Living NT Values
- Privacy Policy
- Employee and Contractor Privacy Policy
- Privacy Breach Policy and Procedure
- Cybersecurity Policy
- Data Governance Policy
- Data Retention and Destruction Policy
- Clinical Governance Policy
- Research Participation Policy
- Discrimination Policy

Healthy Living NT acknowledges that AI technology is rapidly changing and developing and may lead to gaps in policy or procedures related to the use of artificial intelligence.

Healthy Living NT will monitor and regularly review policies and procedures relating to the parameters of use of AI technology within the organisation.

5. Accountability in Decision-Making

The Board has defined acceptable uses of AI at Healthy Living NT through its policy: *Acceptable Use of Artificial Intelligence Tools and Models.*

Healthy Living NT's Board seeks to uphold high standards of ethical behaviour in executing its fiduciary duty. It must avoid conflicts of interest and prioritise the best interests of the community.

The Board is responsible to understand and oversee the legal and ethical implications of AI deployment and to ensure AI use within the organisation is managed in a manner that promotes Healthy Living NT Values. At the request of Board, the Governance Policy Committee may additionally identify and assess risks associated with the use of artificial intelligence or recommend policy enhancements related to use of AI.

The CEO is responsible for presenting the due diligence data related to any new use of AI in the organisation for Board approval prior to use.

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

Approval

Original Submission Date:	Board Meeting 6/24 of 14 December 2024
Original Approval Date:	Board Meeting 6/24 of 14 December 2024

Circulation:	All HLNT Board Members and staff.
Sign off by:	Chair of the Board

Signature: William De Decker

Supporting Policies, Procedures and Documents

HLNT Acceptable Use of Artificial Intelligence Tools and Models
HLNT Ethical Practice Guide
HLNT Values
HLNT Privacy Policy
HLNT Employee and Contractor Privacy Policy
HLNT Privacy Breach Policy and Procedure
HLNT Cybersecurity Policy
HLNT Data Governance Policy
HLNT Data Retention and Destruction Policy
HLNT Clinical Governance Policy
HLNT Research Participation Policy
HLNT Discrimination Policy
HLNT Consumer Charter

Acceptable Use of Artificial Intelligence Tools and Models

1. Purpose

The purpose of this policy is to establish guidelines for the use of an artificial intelligence language model (AILM) including generative AI tools such as ChatGPT (OpenAI), Gemini (Google), CoPilot/Bing (Microsoft/OpenAI) or other similar tools by employees or contractors of Healthy Living NT.

This policy is designed to ensure that the use of AI is ethical, lawful, responsible and in compliance with all applicable laws, regulations and HLNT policies.

2. Scope

This policy applies to all employees, contractors or third parties with access to AILM, doing business on behalf of HLNT, whether through HLNT-owned or BYOD (bring your own device.)

3. Background

Artificial Intelligence (AI) tools are transforming the way we work. They have the potential to automate tasks, improve decision-making and provide valuable insights into our operations.

However, the use of AI tools also presents new challenges in terms of information security and data protection. This policy is a guide for employees to understand:

- how to be safe, secure and ethical when using AI tools,
- potential uses of AI tools within the HLNT environment
- the risks of using AI tools
- information or uses which are excluded from use with AI tools

4. Common Terms

Artificial intelligence	refers to technologies that enable machines to perform tasks traditionally associated with human intelligence, including making content, predictions, recommendations or decisions.
Artificial neural networks	are computing systems that are loosely inspired by the human brain and which consist of interconnected units (or artificial neurons) that are often organised into layers
Machine learning	refers to techniques used in the field of artificial intelligence to enable computer programs to learn from training data rather than relying on predefined rules.
Deep learning	is a subset of machine learning that involves training artificial neural networks to model and solve complex problems. The word 'deep' signifies the fact that these artificial neural networks typically have many layers of neurons.
Large language models (LLMs)	are artificial neural networks trained on vast quantities of text data, often sourced from the internet.
Generative AI	is a term used to refer to new artificial intelligence products like ChatGPT and image generation that can create new, and often creative, content (as opposed to AI tools that focus on other tasks like analysis or classification).

Darwin
Shop 1-3 Tiwi Place,
Tiwi NT 0810
PO Box 40113,
Casuarina NT 0811
Phone: 08 8927 8488
Fax: 08 8927 8515
E: info@healthylivingnt.org.au

Alice Springs
Jock Nelson Centre,
7/16 Hartley Street,
Alice Springs NT 0870
Phone: 08 8952 8000
Fax: 08 8952 7000
E: alicesprings@
healthylivingnt.org.au

www.healthylivingnt.org.au
ABN 11 374 693 055

5. Risks

The use of AILM has inherent risks that employees should be aware of. These risks include, but are not limited to:

- **Confidentiality**: Information entered into an AILM may enter the public domain. This can release non-public information and breach regulatory requirements, customer or client health or personal information, vendor contracts or compromise trade secrets.

  Employees should use AILM responsibly and ethically, in compliance with HLNT Values and policies and applicable laws and regulations.

- **Accuracy**: AILM that relies upon algorithms to generate content. As with AILM technology, there is a risk that AILM may generate inaccurate or unreliable information. Employees should exercise caution when relying on AILM generated content and should always review and edit responses for accuracy before utilising the content.

- **Bias:** AILM may produce biased, discriminatory or offensive content. Employees should use AILM responsibly and ethically, in compliance with HLNT Values and policies and applicable laws and regulations.

- **Security:** AILM may store sensitive data and information, which could be at risk of being breached or hacked.

- **Plagiarism and copyright:** There is a potential risk of inadvertently using copyrighted material or committing plagiarism when utilising AI models, which could lead to serious legal consequences.

While it may prove to be an extremely useful tool, AILM tools have several limitations that may result in undesirable results if inappropriate reliance is placed on it. These limitations include:

HALLUCINATIONS	AILMs are programs that generate text based on statistical models of language. They are not grounded in, or constrained by, any concept of truthfulness, common sense or rules of logic. As a result, AILMs are notorious for generating what some have labelled '*confidently worded bullshit*' (sometimes also referred to as a hallucination). As this output is generated with confidence and without acknowledging any sources, **it can be challenging for users to identify the errors.**
UNRELIABLE	AILMs are unreliable. Not only do they rely on statistical models of language, but there is also an element of randomness incorporated into every output, which means that identical inputs can result in different outputs. This means, for example, that ChatGPT can perform a task correctly on the first nine attempts and then fail catastrophically on the tenth attempt.
FAILS AT CERTAIN TASKS	AILM tool fluency and confident tone can generate the illusion that it possesses some underlying general intelligence. However, there are some tasks in which ChatGPT and other models are incredibly flawed. For example, even the latest version of ChatGPT's large language model (GPT-4) consistently fails in basic tasks like counting and arithmetic. This is because the underlying language model that underpins it is based on probability – it is not a calculator or some kind of inference engine that applies logical rules.

OUTDATED CONTENT	AILM tool training may be based on datasets that are not current. As a result, it may struggle with facts that occurred after that date. OpenAI has recently announced a web browsing plugin that will allow ChatGPT to search the web; however, as this does not involve updating the underlying LLM, it remains unclear to what extent the web browser plugin will resolve issues caused by the limited currency of the dataset.
LIMITED ACCESS TO SPECIALIST INFORMATION	Most AILM tools underlying model were largely trained on publicly available internet resources. Organisations that wish to adapt the tool to use their internal knowledge bases (e.g. to create customer service chatbots) will need to integrate this knowledge via the APIs - a task which might be easier said than done.
TOXICITY AND BIAS	The outputs of AILMs reflect the biases in their training materials. ChatGPT's initial training materials included large portions of the internet and, as such, it sometimes produces extremely toxic and discriminatory output. Although OpenAI has put in place some measures to address this issue (including through content filtering and by specifically training ChatGPT to avoid toxic output), it will be difficult to fully resolve these issues given the statistical nature of LLMs. In fact, attempts to train ChatGPT to avoid toxic and biased outputs give rise to their own issues, as this involves training by humans, each of whom will necessarily have their own biases.
CONFIDENTIALITY AND PRIVACY	Conversations with AILM tools using the consumer-facing product may be used to improve and train future versions of the product. A recent bug in the ChatGPT application allowed some users to view the titles of other users' conversation histories. So, it would be a mistake to input any confidential, sensitive or personal information into the publicly accessible version of ChatGPT right now. OpenAI has recently announced that it will no longer use data submitted through the APIs for training purposes. However, organisations will still need to consider data and privacy issues (including data security and cross- border data transfers).

6. Acceptable use of AILM at Healthy Living NT

The following guidance outlines the requirements that employees must follow when using AI tools, including the evaluation of security risks and the protection of personal, health and other confidential data.

If you have any doubts about using AI to complete a task, please seek advice from your manager.

a) Use of AILM:

Employees are authorised to use AILM tools for acceptable work-related purposes on the following conditions:

- Acceptable purposes include tasks such as:
  - ➢ Generating preliminary text or content for reports, articles, presentations, images and communications of a non-confidential nature which must then be substantially transformed or developed by an employee.
  - ➢ Reviewing text of a non-confidential nature that contains no personally identifiable information.
- Before using any generative AILM tool for any HLNT business, you must opt out of letting generative AI tools use any data you feed the tool to train their AI models. (Opt out for OpenAI via this link).

- If you use AI for authorised HLNT business, you must use accounts created with HLNT email addresses/credentials.
- Acceptable AILM tools include: ChatGPT (OpenAI), Gemini (Google) and Copilot/Bing (Microsoft)
- Any content initially generated with AI assistance must be reviewed by the responsible team members for potential risks, including language issues, bias, and discrimination, confidentiality and plagiarism etc.

b) Unacceptable use of AILM or AI systems:

AI should not be used to compose entire works that are meant to represent the unique intellectual contribution of the employee or Healthy Living NT.

It is expressly forbidden to use any of the following information in association with an AILM:

- Database information (e.g. TM2, Nookal, Membership database etc) must never be provided to an AILM
- Client and doctor letters/communications which contain personally identifiable information should not be provided to an AILM for assistance.

It is expressly forbidden to use AI systems for the automated delivery of services or recommendations to customers or clients or for screening, assessment or decision making in respect of clients or employees.

c) Confidentiality:

Confidential information must not be entered into an AILM tool, as information may enter the public domain.

Confidential information is defined in HLNT's Data Governance Policy as Restricted and Highly Restricted data. It includes, but is not limited to, employee, customer or client health, personal or financial information, HLNT proprietary or financial information including contracts and business models.

Employees must follow all applicable data privacy laws and HLNT policies when using AILM.

d) Ethical Use:

AILM must be used ethically and in compliance with all applicable laws, regulations and HLNT policies and Values.

Employees must not use AILM to generate content that is discriminatory, offensive, or inappropriate. If there are any doubts about the appropriateness of using AILM in a particular situation, employees should consult with their supervisor.

e) Copyright:

Employees must adhere to copyright laws when utilising AILM. It is prohibited to use AILM to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material.

If an employee is unsure whether a particular use of AILM constitutes copyright infringement, they should contact their supervisor for guidance.

f) Accuracy:

All information generated by AILM must be reviewed and edited for accuracy prior to use. Employees are responsible for the outputs generated by AI, including correcting biases and inaccuracies.

g) Acknowledgement:

Content substantially produced via AILM must be labelled or footnoted as containing AILM information. Clearly disclose the use of AI in public communications and to stakeholders.

Compliance

Any violations of this policy should be reported to your supervisor, the Information Services Officer or the CEO. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

Review

This policy will be reviewed periodically and updated as necessary to ensure continued compliance with all applicable laws, regulations and company policies.

Acknowledgment

By using AILM, employees acknowledge that they have read and understood this policy, including the risks associated with the use of AILM. Employees also agree to comply with this policy and to report any violations or concerns to their supervisor, the Information Services Officer or the CEO.

Responsibility for Policy

The Board of Diabetes Association of the NT Inc. is responsible for ensuring this policy is up to date and complied with.

Approval

Original Submission Date: Board Meeting 6/24 of 14 December 2024
Original Approval Date: Board Meeting 6/24 of 14 December 2024

Circulation: All HLNT Board Members and staff.
Sign off by: Chair of the Board

Signature: William De Decker

Supporting Policies, Procedures and Documents

HLNT Artificial Intelligence Governance Framework
HLNT Ethical Practice Guide
HLNT Values
HLNT Privacy Policy
HLNT Employee and Contractor Privacy Policy
HLNT Privacy Breach Policy and Procedure
HLNT Cybersecurity Policy
HLNT Data Governance Policy
HLNT Data Retention and Destruction Policy
HLNT Clinical Governance Policy
HLNT Research Participation Policy
HLNT Discrimination Policy
HLNT Consumer Charter