PRIVACY POLICY:

1. Policy Statement

SNPHNLtd (**SydneyNorth Health Network – "SNHN")** is committed to protecting the privacy of the personal information and sensitive information which it collects and holds. We gather such information to allowusto meet our objectives of improving our community's access to primary health care services.

SNHN is committedtothe protection of all personal, health, sensitive and non-personal information collectedfor the activities and functions of the organisation (including research) and takes proactivesteps to establish and maintain internal practices that ensure compliance with the *AustralianPrivacy Principles* under the Privacy Act 1988 (Cth).

2. Purpose

Thepurposeof this Privacy Policy is to explain:

- theapplication of this Privacy Policy to the activities of SNHN
- thekinds of information which SNHN may collect about our clients, employees, contractors and others and how that information is collected and used
- howSNHN can disclose the information so collected
- howindividuals can access the information held; and
- theprocesses by which SNHN protects the personal information held.

3. Scope

Thispolicy applies to all activities conducted by SNHN and to the actions of its directors, employees, contractors and volunteers.

4. Definitions

InthisPrivacyPolicy, the following terms have the following meanings:

health information is:

- personal information or an opinion about:
  - an individual's physical or mental health or disability (at any time)
  - an individual's express wishes about the future provision of health services for themselves or
  - a health service provided, or to be provided, to an individual
- other personal information collected to provide, or in providing a health service

personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not

sensitive information means

- information or an opinion (that is also personal information) about an individual's:
  - racial or ethnic origins
  - political opinions
  - membership of a political association
  - philosophical beliefs
  - religious beliefs or affiliations
  - sexual orientation or practices
  - criminal record
  - membership of a professional or trade association or
  - membership of a trade union
  - health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification or
- biometric templates

5. How SNHN Addresses the Australian Privacy Principles

Overview

SNHN handles all personal information and sensitive information in a manner which complies with the Australian Privacy Principles. We obtain consent (written or verbal) to collect, store, use and/or disclose this information. SNHN will only collect personal information:

- after a person has consented
- when any secondary use is related to the main reason for collection of personal information;
- for approved research projects or
- in circumstances in which collection is necessitated by the public interest such as law enforcement or public or individual health and safety.

SNHN takes reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date and to protect the personal information it holds against loss, unauthorised access, use, modification or disclosure and against other misuse. SNHN will ensure ethics approval is sought from a registered Human Research Ethics Committee (HREC) for relevant research projects as appropriate.

6. Responsibilities

The Australian Privacy Principles

Part 1 – Consideration of personal information privacy

APP1: Open and transparent management of personal information

SNHN will only collect personal information necessary to undertake our programs, activities or functions. This is managed in an open and transparent way by the maintenance of processes which

- make sure that each individual providing personal information is informed about and understands the purpose of collecting the information,
- disclose to whom and under what circumstances that personal information may be disclosed to another party; and
- allow and provide an individual access to the information held about that person.

This policy will be made available to any person upon request to the Privacy Officer. A general statement describing our approach to privacy is accessible to the public via the SNHN website.

SNHN welcomes queries and feedback from individuals regarding our systems and processes for the collection and management of personal information. Individuals may also wish to contact us for the purposes of correction of personal information (See APP13 below). Such enquiries should be directed to:

The Privacy Officer, Sydney North Health Network
Phone – 02-9432-8250
Email – feedback@snhn.org.au

APP2: Anonymity and pseudonimity

SNHN allows individuals the option of not identifying themselves when providing information except when:

- SNHN is required by law or court tribunal order to deal with persons who have identified themselves or
- it is impractical for SNHN to deal with individuals who have not identified themselves or have used a pseudonym.

Part 2 – Collection of personal information

APP3: Collection ofsolicitedpersonalinformation

SNHN will only collect personal information that is reasonably necessary to provide a service.

SNHN will make sure that each individual who provides personal information is informed about and understands the purpose of collecting the information and its intended use/disclosure.

APP4: Dealing with unsolicited information

SNHN will not keep personal information received about an individual, unless that person has given permission.

SNHN will from time to time collect commercial information that is already available in the public domain. This includes operating details of primary healthcare providers in the region.

SNHN will seek to preserve the accuracy of this information.

APP5: Notification of the collection of personal information

When collecting personal information about an individual, SNHN will first inform the individual of the purpose of collection and to whom or under what circumstances their personal information may be disclosed to another party.

Part 3 – Dealing with personal information

APP6: Useof and disclosure of personal information

SNHN willonly use personal information for the purpose for which it was collected or that would reasonablybe expected by the individual providing the information.

SNHN will only disclose personal information without consent where such disclosure is required by law, or for law enforcement, or in the interests of the individual's or the public's health and safety.

Individuals will be given the opportunity to refuse such use or disclosure. If an individual is physically or legally incapable of providing consent, a responsible person (as described under the Privacy Act 1988) may do so.

SNHN will keep records of any such use and disclosure. Information may only be disclosed to a responsible person (as described under the Privacy Act 1988).

Information sharing for continuity of health care shall be with authorised individuals and organisations on a need to know basis, and, be directly relevant to the client's continuity of health care.

If information is to be used for a secondary or unrelated purpose, such as service evaluation, SNHN will obtain further consent unless the data will be de-identified i.e. elements of the data will be removed or substituted to ensure that an individual's identity cannot be readily determined or recognised.

6.1 Use or Disclosure of Sensitive (Health) Information

Health information will not be used for a secondary purpose without the express consent of the individual.

Health information will only be disclosed to a third party for a secondary purpose in the following circumstances:

- with the express consent of the individual; or
- where there is a reasonable belief that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare, or a serious threat to public health or safety.

APP7: Direct marketing

SNHN will not provide personal information to another person or organisation for direct marketing except:

- with the express consent of the individual in circumstances where that specific use of the information is intended; or
- when the organisation is a contracted service provider to the Commonwealth and the disclosure of the information is necessarily required to meet an obligation under that contract.

APP8: Cross-border disclosure

SNHN will not provide personal information overseas unless legally required to do so

APP9: Adoption, use or disclosure of Government related identifiers

SNHN will not use any Government related identifier (eg Medicare or Veterans' Affairs numbers or similar) as our identifier, nor will we disclose it.

Part 4 – Integrity of personal information

APP10: Quality of personal information

SNHN takes reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Consumers and stakeholders are invited to contact us if they become aware that the information, we hold on them is inaccurate or out of date.

APP11: Security of personal information

SNHN takes care to protect and hold securely personal information whether electronic or on paper. All data resides on SNHN systems either onsite or cloud based (hosted in Australia) but not as part of share cloud service (with the exception of data hosted in a secure manner on the Primary Health Insights platform).

All personal information held by SNHN will be:

- if in paper form, received and stored in a secure, lockable location,
- if in electronic form, password and firewall protected, and externally backed up with a provider contractually bound to confidentiality,
- accessible by employees only on a "need to know" basis, and
- not taken from the SNHN offices unless authorised and for a specified purpose.

SNHN destroys or permanently de-identifies personal information that is no longer required to be held.

Board members, employees, volunteers (including students) contracted agents and service providers have been informed of the importance of protecting information privacy and their role in helping us do so. All are required to adhere to SNHN's Code of Conduct (or Board Code of Conduct if applicable), this Policy and other policies and procedures relating to the use and disclosure of personal information. All SNHN employees must, under their contract of employment, adhere to confidentiality requirements and privacy obligations related to the use of information which has been disclosed to or acquired or by the employee during the course of their employment. Further, contracting parties may be required to sign a confidentiality agreement upon their engagement by or in their other involvement with SNHN.

Part 5 – Access to and correction of personal information

APP12: Access to personal information

Individuals may request access to their own personal information. Access will be provided unless there is a sound reason under the Privacy Act 1988 or other relevant law to withhold access.

Situations in which access to information may be withheld may include when:

- there is a threat to the life or health of an individual,
- access to information creates an unreasonable impact on the privacy of others,
- the request is clearly frivolous or vexatious or access to the information has been granted previously,
- there are existing or anticipated legal dispute resolution proceedings, and
- denial of access is required by legislation or law enforcement agencies.
- SNHN suspects unlawful activity or conduct of a serious nature.
- giving access would reveal evaluative information within SNHN in connection with a commercially sensitive decision-making process

SNHN responds to a request to access or amend information within 30 business days of receiving the request.

APP13: Correction of personal information

We will correct the personal information we hold about a person if it is inaccurate, out of date, incomplete or misleading.

Amendments may be made to personal information to make sure it is accurate, relevant, current, complete and not misleading, taking into account the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, SNHN may refuse the request.

If the requested changes to personal information are not made, the individual may make a statement about the requested changes and the statement will be attached to the record.

SNHN will respond to queries and requests for access and amendment to personal information within 30 days by electronic means or by registered post correspondence. To request access to personal information for the purposes of correction, individuals should contact:

The Privacy Officer, Sydney North Health Network
Phone – 02-9432-8250
Email – feedback@snhn.org.au

7. SNHN Data Register and Data Set Privacy Impact Assessment Process

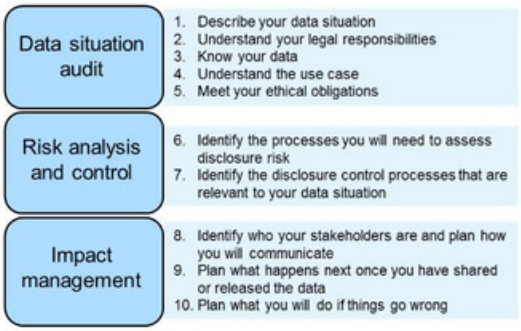
The organisation will maintain a data asset register which is a repository of all SNHN Data Sets (**SNHN Data Register**) incorporating the following for each Data Set:

- Name and description (including purpose)
- Date of commencement and duration of use
- Data classification
- Data specific roles including business and IT owners, data sponsor, data custodian, data steward
- Data management including- data extraction, data dictionary/meta data and other supporting documentation
- Key risks and controls
- Privacy Assessment outcome
- Data quality

The SNHN Data Register is updated as required by the business owner and reviewed annually by the Data Governance Committee for their compliance with the Australian Privacy Principles.

The sharing of data by SNHN occurs on diverse platforms, including a shared data platform. A key starting point is the use of the Data Set Privacy Impact Assessment process to allow for the understanding of any privacy related obligations for that data set, including conditions for sharing. For example, whether data is de-identified, under what conditions it remains de-identified, and how to determine the conditions under which data could be safely shared.

Atemplate outlining the 10 components of the *Data Set Privacy Impact Assessment* process iscompleted for each Data Set. These ten components are set out below[1]:



[1] *Data Set Privacy Impact Assessment toolset's use of the De-identification Decision-Making Framework*

8. Confidentiality of other Information

All information held by SNHN in the course of its activities is confidential. It is appropriate that a decision to release or make public (e.g. website content) gives due consideration to confidentiality of the information and the appropriateness of wider distribution.

If they are unsure whether information is confidential to SNHN or its clients, employees and stakeholders are to refer to the CEO or Privacy Officer before transferring or providing information to an external source.

9. Breach of privacy or confidentiality

Employees who are deemed to have breached privacy standards set out in this policy may be subject to disciplinary action as described in SNHN Code of Conduct.

If a client or stakeholder is dissatisfied with the conduct of a SNHN employee or director, this should be raised with the Privacy Officer.

Notifiable Data Breaches

Under the notifiable data breaches (NDB) scheme, which was established following the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, SNHN is required to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm and the Australian Information Commissioner (Commissioner) in the case of 'eligible data breaches'.

SNHN has put in place a Data Breach Response Plan which sets out the procedure to be followed by SNHN employees in the event that SNHN experiences a data breach, or suspects that a data breach has occurred.

[1] The ten components are discussed in the *De-identification Decision-Making Framework (DDF*) released by the Office of the Australian Information Commissioner (OAIC) and Commonwealth Scientific and Industrial Research Organisation (CSIRO)'s Data61 in 2017.

10. Responsibilities

Chief Financial Officer

The CFO is SNHN's Privacy Officer. The CFO is the contact point for all privacy and confidentiality related enquiries and issues (from both external and internal parties). Privacy enquiries can be made by:

- Phone – 02-9432-8250
- Email – feedback@snhn.org.au
- Website - https://sydneynorthhealthnetwork.org.au/

The CFO is responsible for the development and implementation of the policies, procedures and other governance tools required to comply with organisational and statutory privacy requirements. This will include ongoing enforcement, monitoring and evaluation of SNHN's privacy processes. The CFO is accountable to the organization's CEO for compliance.

Employees and directors

Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information.

Understand the organisation's ethical standards regarding the treatment of other confidential information relating to SNHN, its clients, employees and stakeholders.

Act in accordance with organisational systems in place to protect privacy and confidentiality. Comply with Privacy Policy, Procedure and associated governance instruments.

11. References

Internal interdependencies

- Code of Conduct
- Information Management Policy
- Information Technology Security Policy
- Recruitment, Selection & Induction Policy & Procedure
- Feedback and Complaints Policy
- Data Breach Response Plan
- SNHN Data Register
- SNHN Privacy Impact Assessment Template
- SNHN Data Governance Framework
- SNHN Data Governance Policy

External interdependencies

- Privacy Act 1988 (Cth) ("Privacy Act") incorporating Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Privacy Principles (Jan 2014)
- Health Care Identifiers Act 2010
- Privacy and Personal Information Act 1998 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- Freedom of Information Act 1989 (NSW)

12. Approvals & Review

Version	Date Approved	Owner (title)	Approver (title)	Next Review Date	Comments
01	*23 Nov 2015*	Lynelle Hales (CEO)	Board	Nov 2018	
02	30 Jan 2019	Lynelle Hales (CEO)	Board	June 2021	
03	3 November 2020	Lynelle Hales (CEO)	Board	Nov 2023	*Reviewed by DGC on 1 October 2020. Reviewed by Clinical Governance Committee on 14 October 2020.*
04	28 February 2024	Kevin Barrow	Board	Nov 2027	*Reviewed by FARM in September 2023 and February 2024 – no substantive changes recommended.*