phn CENTRAL AND EASTERN SYDNEY
An Australian Government Initiative

Privacy Policy

Version	**2.0**
Document Author	General Manager – Corporate Services
Approved By	Board
Effective Date	26 September 2023

Contents

Purpose

This policy provides guidance on EIS Health Limited (trading as Central and Eastern Sydney Primary Health Network - CESPHN) legal obligations and ethical expectations in relation to privacy. This policy outlines how CESPHN handles personal information and health information and how we comply with our privacy obligations. CESPHN updates this policy if anything changes, and a full review is completed every two years.

CESPHN is bound by the Australian Privacy Principles (APPs) as set out in the *Privacy Act 1988 (Cth)* as well the *Health Records Information Privacy Act 2002 (NSW)* and other contractual agreements that impose specific obligations in relation to personal and health Information that directly or indirectly identifies a person.

The Privacy Act also prescribes the APPs which regulate the collection, use, disclosure, management and storage of personal information. It also provides guidance for individuals accessing and correcting their own personal information.

CESPHN acknowledges good privacy practice is more than being compliant with the Privacy Act and other legislation. Any mishandling of personal information may result in a loss of trust in CESPHN by our stakeholders and cause significant harm to our reputation.

Legislation

- Privacy Act 1988 (Cth), which includes the *Privacy Amendment (Notifiable Data Breaches)* and the Australian Privacy Principles (APP). The APPs regulate the handling of personal information.
- Data Availability and Transparency Act 2022 (Cth)
- Health Records and Information Privacy Act 2002 (NSW).

Definitions

Term	Definition
Consent	Consent has four key elements: • the consent must be voluntary • the individual must be adequately informed before giving consent • the consent must be current and specific • the individual must have the capacity to understand and communicate their consent.
Health information	In accordance with section 6 of the Privacy Act, information or an opinion about: 1) the health or a disability (at any time) of an individual; or 2) an individual's expressed wishes about the future provision of health services to themselves; or 3) a health service provided, or to be provided, to an individual; or 4) other personal information collected to provide, or in providing, a health service; 5) other personal information about an individual collected in connection with a donation,

	or intended donation, by the individual of their body parts, organs or body substances; or 6) genetic information about an individual in a form that is or could be, predictive of the health of the individual or a genetic relative of the individual.
Privacy	Refers to the right of individuals to control how their information is collected, stored and used.
Privacy Officer	The General Manager – Corporate Services, responsible for Privacy concerns/issues at CESPHN.
Personal information	Means information about an individual whose identity is apparent, or can reasonably be ascertained, from the information, which is maintained electronically, on video, in photographs or in written/printed form and/or verbal information given to an employee about an individual.
Sensitive information	Includes information or an opinion about an individual's: • racial or ethnic origins • political opinions or membership of a political association • religious beliefs or affiliations • philosophical beliefs • membership of a professional or trade association or membership of a trade union • sexual preferences or practices • criminal record • health, genetic or biometric templates, that is also personal information.
Staff	• Any person performing work for CESPHN. All board directors, board sub-committee members, executives, employees, contractors, consultants, students and researchers (including visiting practitioners, agency staff, staff employed by partnering organisations and persons delivering training or education to or for CESPHN) are Staff for the purposes of this policy to the extent that they contribute to work interests.
Stakeholders	• Anyone external to our organisation that has a relationship with CESPHN. Including but not limited to: commissioned service providers, advisory committees members, stakeholder working groups, the community and tender panel members.

Policy scope

This policy applies to all CESPHN Staff who have access to personal information while performing their duties and all individuals whose personal information is collected by CESPHN.

The Privacy Act defines personal information as:

'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'.

Personal information does not include, and is not, information already and lawfully in the public domain including generally available documents including annual reports, newsletters, magazines, books and newspapers.

Policy statement

CESPHN is committed to treating the personal information we collect in accordance with the Australian Privacy Principles (APP) in the Privacy Act 1988 (Cth) the ("Act") and the Health Records and Information Privacy Act 2002 (NSW).

CESPHN will protect the privacy of its Staff, of people accessing its services, of its members, and of any other stakeholders and members of the community on whom it possesses personal information.

Compliance with Australian Privacy Principles

CESPHN complies with APPs, as follows:

- **Open and transparent management of personal information** – personal information is managed in a robust and transparent way, through implementation of this policy and supporting frameworks.
- **Anonymity and pseudonyms** – individuals have the option to not identify themselves, or to use an alternate name when dealing with CESPHN in relation to certain matters, where it is lawful and practicable to do so.
- **Collection of solicited personal information** – personal information is collected through lawful and fair means only where it is reasonably necessary for, or directly related to, its functions and activities.
- **Dealing with unsolicited personal information** – unsolicited personal information received but not collected through normal processes, will be de-identified or destroyed where lawful and reasonable to do so.
- **Notification of the collection of personal information –** individuals are notified when CESPHN is collecting personal information.
- **Use or disclosure** – personal information is only collected and used for specified purposes. Personal information is de-identified where possible when it is disclosed.
- **Direct marketing** – personal information is not used for direct marketing unless authorised by the individual concerned.
- **Cross border disclosure of personal information** – personal information is not disclosed to overseas recipients.
- **Use or disclosure of government related identifiers** – government related identifiers are not released by CESPHN in its use or disclosure of personal information.
- **Quality of personal information** - reasonable steps are taken to ensure personal information collected is accurate, up to date and complete.
- **Security of personal information** – appropriate steps are taken to ensure personal information is protected from misuse, interference, loss, unauthorised access, modification and disclosure.
- **Access to personal information** - access is provided to an individual to their personal information held by CESPHN as required by the Privacy Act.
- **Correction of personal information -** an individual is able to request corrections to their personal information held by CESPHN as required by the Privacy Act.

Collection of Personal Information

Personal information is only collected as necessary to either facilitate, manage or deliver health services and to improve the coordination and delivery of health services.

CESPHN will take reasonable steps to ensure an individual's personal information is accurate, complete and up-to-date.

The type of information collected may include:

- Identifying information such as name and former names, date of birth, place of birth, employment details, cultural identity and qualifications
- Contact information such as home address, mobile phone numbers, emergency contact numbers and email addresses
- Government-issued identifiers including Medicare numbers
- Financial information such as bank account and credit card details
- Sensitive information that may include information about an individual's health and health services provided to the individual.

CESPHN may also keep personal information as part of the following records:

- Recruitment and Human Resources
- Board membership
- Advisory Committee membership
- Information systems/Client Information Systems, compliance, and contract management systems.
- Correspondence and Stakeholder Management/CRM
- Financial management and administration
- Incident records regarding the performance of its functions and activities, such as workplace incidents
- Notifiable Clinical Incidents reported by service providers
- Event Management and attendance
- Right to Information, Complaints, Privacy, and Litigation records.

CESPHN may also need to collect Health Information as is necessary to provide or assist in the Commissioning of the provision of primary health care services and for the purpose of understanding the CESPHN region's health needs particularly in relation to vulnerable populations including but not limited to people from Multicultural backgrounds, people living with a disability, people from the LGBTIQ+ community and Aboriginal and/or Torres Strait Islander peoples.

All clinical information will be de-identified unless consent is provided by the individual and falls outside the provisions of the Privacy Act dealing with Health Information.

CESPHN may also collect personal information from public sources (e.g., national health practitioner register, internet), or through memberships (e.g., with peak bodies or accreditation agencies), to understand compliance against standards or population health needs.

Sometimes Health Information may be collected from a third party such as a health service provider. Where it is lawful and practicable, individuals in dealing with CESPHN, will have the option of not having to identify themselves but only where such anonymity or pseudonymity will not compromise or prevent CESPHN from effectively carrying out its activities and functions.

CESPHN will collect information on the basis of it being lawful and fair and will take measures to ensure each individual providing personal information is informed, and understands, the purpose of the collection of the information and, where possible, CESPHN will require the informed consent of an individual giving personal information.

Use and disclosure of Personal Information

CESPHN will only use personal information for the purpose it has been given, usually directly from individuals and their representatives unless it is unreasonable or impractical to do so.

The following exceptions apply**:**

- Another purpose is directly related to the purpose for which information was given to CESPHN and it would be reasonably expected that this information would usually be disclosed for another purpose or to other individuals, organisations or agencies.
- CESPHN is required or authorised by law to disclose information for another purpose or disclosure is reasonably necessary for the enforcement of law.
- The disclosure of information will prevent harm or injury to a person.

CESPHN collects health and sensitive information with the informed consent of the individual. Consent is collected in writing where possible, using a purpose-specific consent form. Where written consent is not possible and verbal consent is obtained, a note including the description of the verbal consent obtained and the date must be made in the client's record in the Client Information Management System.

CESPHN may also provide Health Information about an individual's condition to parents, children, other relatives, close personal friends, guardians, or a person exercising a power of attorney under an enduring power of attorney, unless CESPHN is expressly informed by the individual there is to be no disclosure of Health Information to that person.

With an individual's consent CESPHN can also use personal information for other purposes including mailing lists, fundraising or research. Unless an individual provides CESPHN with their express consent for this purpose, CESPHN will not use personal information in this way.

Access to Personal Information

Requests by individuals to access their personal information held by CESPHN must be in writing to the relevant Data Custodian or Steward. CESPHN will respond to requests for access to personal information within a reasonable period and there will be no charge for the provision of an individual's information, except in circumstances where CESPHN incurs a cost.

CESPHN Staff may require some identification to prove that the individual has the right to access the information or is authorised by a third-party to access the information.

CESPHN Staff will clearly state in writing that approval has been granted to release the personal information, stating the individual's full name. The approval will be saved against the relevant record.

Access must be provided unless one of the exceptions under the Privacy Act applies. CESPHN is not required to provide an individual access to their personal information in the following circumstances:

- CESPHN reasonably believes that giving access may pose a serious threat to the life, health or safety of any individual, or public health or public safety, or is unlawful or in contravention of a court order.
- Access to the information would have an unreasonable impact on the privacy of others.
- The request for access is frivolous or vexatious.
- There are existing or potential legal proceedings occurring between CESPHN and the individual, and the information would not be accessible through the legal discovery process.
- CESPHN suspects unlawful activity or misconduct may have been engaged in relating to CESPHN's functions and giving access to the information may prejudice

taking appropriate action in relation to the matter.
- Giving access would be likely to prejudice enforcement related activities conducted by or on behalf of an enforcement body.
- Giving access would reveal evaluative information generated within CESPHN relating to commercially sensitive decision-making process or would reveal CESPHN's intentions in any negotiations with any individual.

Correction and transfer of Personal Information

CESPHN will correct the personal information of an individual if it is inaccurate, out of date, incomplete or misleading.

- All requests to correct or transfer personal information by an individual held by CESPHN must be in writing to the relevant Data Custodian or Steward. The Data Custodian or Steward is responsible for actioning all requests, including:
- liaising with other internal staff members
- keeping a record of the request
- making a copy of the record, and
- securely transmitting a copy of the record as required.

CESPHN will transfer personal information (e.g., to a new health provider) if it is requested by the individual and consent is provided.

Third parties are not permitted to access or correct the record of another individual without written consent, signed by a Justice of the Peace or other authorised person (e.g., Guardian). The following exceptions to third party release of information may apply:

- If the information is requested via a subpoena
- In accordance with provisions set forth by the Office of the Information Safety Commissioner, emergency access may be granted to a third party (e.g., hospital or police) if it is not reasonable or possible to gain the consent of the consumer.

This is reserved for exceptional circumstances where there is reason to believe that access to the information will lessen or prevent a serious threat to the life of the consumer, or serious health and safety risk.

All requests for personal information received via subpoena or an emergency access request must be referred to the stream General Manager and the Privacy Officer for action.

Before giving an individual access to health information, CESPHN Staff must take reasonable steps to be satisfied about that person's right to the information and, for this purpose, may require evidence of:
- the person's identity
- if an individual has authorised the organisation to provide access to that person, the authority of the individual, and
- if the person seeking access is an authorised representative of the individual, or the legal representative of a deceased individual.
-
- If there has been a data breach, please contact the Privacy Officer and refer to the section below '*Data Breaches and Notifiable Data Breaches'.*

Refusal of access or correction of Personal Information

- CESPHN may refuse to grant access or correct an individual's personal information to some or all of the record, if doing so could potentially pose a serious threat to the life or health of the individual or any other person.
-

The Privacy Officer will make a recommendation to refuse access to the relevant General Manager. The General Manager is responsible for making a final decision to refuse access.

In such situations the Privacy Officer will provide the individual with written notice that sets out:

- the reasons for the refusal, and
- the mechanisms available to the individual to make a complaint.

Storage and disposal of Personal Information

CESPHN Staff take steps to protect an individuals' personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.

CESPHN protects and holds securely personal information whether electronic or on paper. All personal information held by CESPHN is:

- If in paper form, received and stored in a secure, lockable location
- If in electronic form, adequately protected according to best practice (in accordance with the CESPHN Cyber Security Policy and Australian Privacy Principles)
- Accessible by staff on a "need to know" basis only and where that access is purposeful, appropriate and legal, and
- Not taken from the CESPHN offices unless authorised and for a specified purpose.

CESPHN securely destroys or permanently de-identifies personal information that is no longer required to be held. Records are kept in accordance with the record-keeping obligations that apply to the category of record. Records are audited quarterly by Staff members to ensure deletion of data where appropriate.

As most CESPHN systems utilise cloud storage solutions, the following principles apply and are adhered to:

- All data is kept on Australian servers where possible, noting that all Health Information CESPHN holds must be stored on Australian servers only and this is documented in all licence/service agreements.
- Cyber security is paramount and security measures around who has access to personal information is restricted by role requirements.
- Additional information about system and data security, including treatment of breaches, is included in the CESPHN Cyber Security Policy and Procedure.

CESPHN will take reasonable steps to destroy or permanently de-identify an individual's information when it is no longer needed. Unsolicited personal information is information provided without it being requested. If CESPHN receives unsolicited personal information that it could not collect through its normal processes, it will be de-identified or destroyed where lawful and reasonable to do so.

Please refer to the Data Governance Framework for specific data disposal requirements relating to Health Information for clinical services.

Data Breaches and Notifiable Data Breaches

A 'Data Breach' occurs where personal information held by CESPHN is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include:

- Lost or stolen laptops or tablets
- Lost or stolen mobile phone devices
- Lost or stolen paper records or documents containing personal information
- Staff mistakenly providing personal information to the wrong recipient
- Unauthorised access to personal information by a Staff member
- Staff providing confidential information to stakeholders
- Credit card information lost from insecure files or stolen from garbage bins
- Where a database has been 'hacked' to illegally obtain personal information, and
- Any incident or suspected incident where there is a risk that personal information may be misused or obtained without authority.

If a Data Breach has occurred, Staff are to immediately complete a Data Breach Notification Folio form and refer to the Data Breach Response Plan.

Staff who are deemed to have breached privacy standards set out in this policy may be subject to disciplinary action as set out in their CESPHN employment contract. The Code of Conduct for the Board outlines requirements for confidentiality and privacy of all information, including commercially sensitive or legally privileged information.

If an individual or organisation is dissatisfied with the conduct of a CESPHN Staff member in regard to a breach of this policy, this should be raised with the Privacy Officer.

A 'Notifiable Data Breach' occurs where there is an actual Data Breach, and:

- a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual including harm to their physical or mental well-being, financial loss, or damage to their reputation; or
- in the case of loss (i.e., leaving an unsecure laptop containing personal information on a bus), unauthorised access or disclosure of personal information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual including harm to their physical or mental well-being, financial loss, or damage to their reputation.

A Notifiable Data Breach does not include a Data Breach where CESPHN has been successful in preventing the likely risk of serious harm by taking remedial action.

Assessment

If CESPHN is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the Data Breach is a Notifiable Data Breach or not.

Notification

Subject to any restriction under the Privacy Act, in the event that CESPHN is aware of a Notifiable Data Breach, CESPHN will as soon as practicable, prepare a statement outlining details of the breach and notify:

- the individual whose personal information was part of the Data Breach, and
- the Office of the Australian Information Commissioner.

Privacy concerns or complaints

If an individual has concerns in relation to the way their personal information has been handled, they are able to contact the Privacy Officer who will liaise with the relevant General Manager.

If CESPHN receives complaints from Stakeholders in relation to the management of personal information, the individual is to refer to CESPHN External Complaints Policy.

If the complaint is of an internal nature, CESPHN Staff members, should refer to the CESPHN Grievance Policy.

Privacy Officer

The General Manager of Corporate Services is the CESPHN Privacy Officer. The Privacy Officer is the contact point for all privacy related enquiries and issues (from both external and internal parties). Privacy enquiries can be made by:

- Phone: 1300 986 991
- Email: info@cesphn.com.au

Policy document control

Documents related to this policy
Clinical Governance Framework
Internet and Computer Usage Policy and Procedure
Clinical Incident Policy and Procedure
External Complaints Policy and Procedure
Grievance Policy and Procedure
Management of Consumer Health Records Policy and Procedure
Identification of Healthcare Consumers Policy and Procedure
Cyber Security Policy
Data Breach Response Plan
Privacy Act 1988 (Cth)
Privacy Amendment (Enhancing Privacy Protection) Act 2012
Australian Privacy Principles
Health Records and Information Privacy Act 2002 (NSW)

Policy review and version tracking

Version	Date Approved	Approved By	Next Review Date
1.0	29 July 2019	EIS Health Limited Board	10 July 2021
2.0	26 September 2023	EIS Health Limited Board	26 September 2025