PRIVACY POLICY AND PROCEDURE

NAME OF POLICY	Privacy Policy and Procedure
VERSION	2
EFFECTIVE DATE	29 July 2019
APPROVED BY	EIS Health Ltd Board
DATE LAST REVIEWED	10 July 2019
SCHEDULED REVIEW DATE	10 July 2021

EIS Health Ltd.

phn CENTRAL AND EASTERN SYDNEY
An Australian Government Initiative

1.0 Purpose

This policy provides guidance on EIS Health's legal obligations and ethical expectations in relation to privacy. This policy outlines EIS Health handles personal information and how we comply with our privacy obligations. We update this policy if anything changes, and fully review it every two years.

Under this policy, we adhere to the:
Privacy Act 1988 (Cwlth) (Privacy Act)
Health Records and Information Privacy Act 2002 (NSW)

2.0 Definitions

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

Means information or an opinion about:

- the health or a disability (at any time) of an individual; or
- an individual's expressed wishes about the future provision of health services to them; or
- a health service provided, or to be provided, to an individual; or
- other personal information collected to provide, or in providing, a health service.

Privacy

Refers to the right of individuals to control how their information is collected, stored and used.

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 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.

3.0 Scope

This policy applies to all activities conducted by EIS Health and to the actions of its directors, employees, contractors and volunteers.

4.0 Policy

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

EIS Health 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.

5.0 Type of information we collect and hold

Health providers and stakeholders

EIS Health collects personal information regarding health providers and stakeholders (for example, general practices, aged care providers, government agencies), and their employees to better understand and improve the health system. The type of information can include name, contact details (address, telephone, email address), role/health services provided, languages spoken, connection with EIS Health.

Consumers

We collect personal details to arrange health services, manage service demand and, in some rare cases, provide a service and maintain client records.

Where EIS Health arranges a health service, we will collect health information and sensitive information. This information is needed to properly triage and refer consumers to an appropriate service and/or contractor. The types of information collected can typically include contact details (name, address, telephone, email address), next of kin/carer, age, date of birth, gender, marital status, Medicare number, NDIS participation, Health Care Card, Medical history, reason for referral, cultural identity.

Website visitors

EIS Health collects and stores information such as individual IP addresses, internet service providers and activity on our website. This information is usually anonymous and we do not use it to identify individuals. However due to the nature of internet protocols, such information might contain details that identify individuals. This information is only used to improve our website and related services.

Prospective employees and directors

EIS Health collects personal information regarding prospective employees and directors, regarding their skills, interests, qualifications and experience to:

- Assess their suitability for potential employment or directorships with us
- Match them to suitable projects

Others

EIS Health may collect personal (including health) information related to the general public in connection with our population planning, research and analysis. This information will generally be de-identified.

We collect the personal information of

- Directors
- Employees
- committee members
- people who have signed releases to take part in photographic, video or audio relating to our work and publications
- subscribers of our publications

- individuals who make a complaint or provide feedback on our work or commissioned services
- individuals who make a request under the freedom for information act
- and others relating to our corporate and other administrative functions.

The type of information collected can include name and former names, contact details (address, telephone, email address), date and place of birth, financial and personal interests which may give rise to conflicts or be required for insurance purposes, bank account details, qualifications obtained.

6.0 How we collect information

We generally collect personal information directly from individuals and their representatives, unless it is unreasonable or impractical to do so. We collect health and sensitive information with the informed consent of the consumer. 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 clients record in the Client Information Management System.'

For some health providers and stakeholders, we may collect personal information from colleagues or other health providers, stakeholders or consumers. In some cases, we collect personal information from public sources (for example national health practitioner register, internet, social media) or through memberships (for example with peak bodies).

7.0 Purpose for which we collect and deal with personal information

As a general principle, we only use personal information for the primary purpose for which we collect the information, or a secondary purpose related to the primary purpose for which it would be reasonable expect us to use the collected information.

We will not use personal information for an unrelated secondary purpose unless we obtain the consumer's written consent or an exception applies, such as it is impracticable to obtain consent and we believe that collecting, using or disclosing personal information is necessary to lessen a serious threat to life, health or safety of any individual.

8.0 How we store information

EIS Health takes care to protect and hold securely personal information whether electronic or on paper. All personal information held by EIS Health 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 EIS Health Cyber Security Policy and Australian Privacy Regulations)
- Accessible by staff only on a "need to know" basis only and that access is purposeful, appropriate and legal; and
- Not taken from the EIS Health offices unless authorised and for a specified purpose.

EIS Health 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.

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

1. All data is exclusively kept on Australian servers and this is documented in all licence/service agreements
2. Cloud security is paramount and security around who has access to and what provisions are available for restoration of data (in the event of accidental or malicious damage) must be obtained and accompany all requests for cloud storage

Additional information about system and data security, including treatment of breaches, is included in the EIS Health Cyber Security Policy and Procedure.

9.0 Cross border transfer or disclosure of information

EIS Health will not provide personal information overseas unless legally required to do so.

10. Access to, transfer and correction of personal information

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.

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.

Transfer of personal information
We will transfer personal information (e.g., to a new health provider) if it is requested by the individual.

Procedure for accessing, correcting or transferring personal information
All requests to access, correct or transfer personal information held by EIS Health, must be referred to the Privacy Officer. The Privacy Officer 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 to the individual.

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:

1. If the information is requested via a subpoena
2. 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 information received via subpoena or an emergency access request must be referred to the General Manager for action.

Before giving a person access to health information, EIS Health personnel must take reasonable steps to be satisfied about that person's right to it 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

Procedure for refusing access to personal information.
EIS Health may refuse to grant access 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
- where information has been given in confidence by a third party (consent from third party must be secured)

The Privacy Officer or other representative 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.

11. 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 set out in their EIS Health 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 an EIS Health Director, employee, contractor or volunteer in regard to a breach of this policy, this should be raised with the Privacy Officer.

12. Privacy Officer

The Human Resources Manager (HRM) is the EIS Health 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

13. Policy document control

Documents related to this policy
Clinical Governance Framework
IT Infrastructure Policy
Clinical Incident Policy and Procedure
Complaints Policy and Procedure
Management of Consumer Health Records Policy and Procedure
Identification of Healthcare Consumers Policy and Procedure
Cyber Security Policy

14. References and Related Documents

- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Australian Privacy Principles (Jan 2014)
- Health Records and Information Privacy Act 2002 (NSW)

15. Policy review and version tracking

Review	Date approved	Approved by	Next review due
10 July 2019	29 July 2019	EIS Health Ltd Board	**10 July 2021**